FIDIS

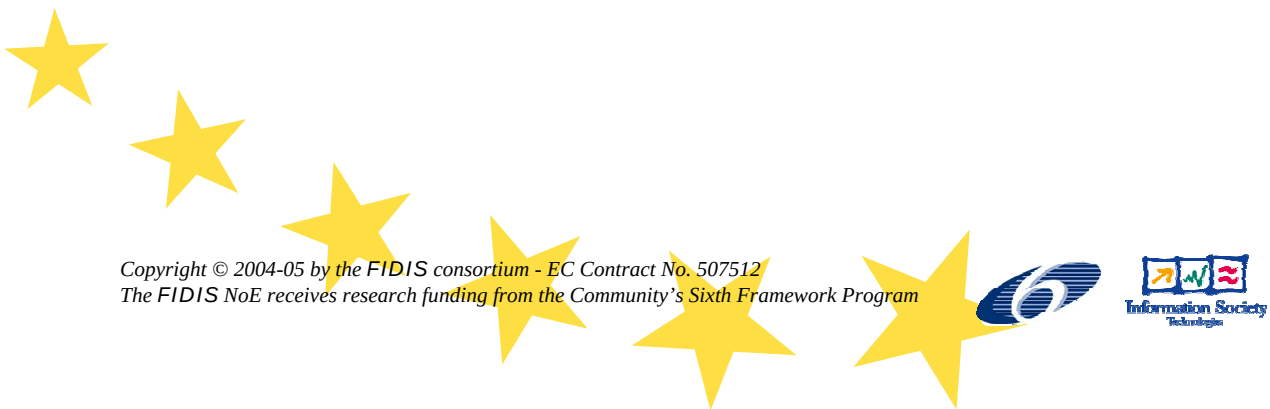
Future of Identity in the Information Society

Title:	"D3.5: Workshop on ID-Documents"
Author:	WP3
Editors:	Martin Meints (ICPP)
Reviewers:	Marit Hansen (ICPP) Xavier Huysmans (Katholieke Universiteit Leuven)
Identifier:	D3.5
Type:	[Report]
Version:	1.0
Date:	Monday, 05 September 2005
Status:	[Final]
Class:	[Public]
File	fidis-wp3-del3.5.workshop_on_id_docs.doc

Summary

The workshop on ID documents was held on June 21st and 22nd, 2005 in Frankfurt, the documentation (agenda, presentations and minutes) can be found at http://internal.fidis.net/200.0.html?&dir=D3.5_Workshop_on_ID_Documents&mountpoint=11.

The preparation of D3.6 "Study on ID Documents" was co-ordinated basing on the exchange of knowledge within the FIDIS NoE and external input provided by two invited speakers.



The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	01.07.2005	Initial release (Martin Meints, ICPP)
0.2	05.07.2005	Conclusions added (Martin Meints, ICPP)
0.3	07.07.2005	Input from Marit Hansen, ICPP
0.4	04.08.2005	Input by K.U.Leuven R&D (Xavier Huysmans)
0.5	15.08.2005	Integrative editing (Marit Hansen, Martin Meints, ICPP)
1.0	16.08.2005	Final additions (Xavier Huysmans, KULeuven) and finalisation of the document (Martin Meints, ICPP)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Workshop on ID Documents)	Martin Meints, Marit Hansen, Xavier Huysmans
2 (Conclusion)	Martin Meints, Marit Hansen, Xavier Huysmans
Annex 1	Martin Meints

Table of Contents

1 Workshop on ID Documents in Frankfurt

1.1 Date and Location

Date:

21st and 22nd of June 2005

Location:

Johann Wolfgang Goethe-University, Frankfurt

Casino Building, room 1.801 and 1.802 (2nd floor)

Grüneburgplatz 1, D-65090 Frankfurt, Germany

1.2 Held Presentations and Additional Information

Material: see presentations on FIDIS webspace http://internal.fidis.net/200.0.html?&dir=D3.5_Workshop_on_ID_Documents&mountpoint=11

1.3 Objectives of the workshop

This workshop had three objectives:

1. To exchange experience about planned or introduced ID documents using new technologies such as electronic signatures, biometrics, and RFID within the FIDIS NoE
2. To get information concerning planned or introduced ID documents from outside the network
3. To organise the content of D3.6 “Study on ID Documents” by discussion of the table of content and co-ordination of the contributions of the partners

To provide an appropriate environment for the three different objectives, the workshop was planned for one and a half days. Day 1 was foreseen for the objectives 1 and 2, including the invitation of two external speakers. The second day was planned for elaborating objective 3 with members from the FIDIS NoE only. Especially those partners were planned to be represented, where the preparation of the workplan showed the need to co-ordinate their contributions.

1.4 Agenda, Minutes and Results, 1st Day

10h00-10h15 Welcome Kai Rannenberg (GUF) and Martin Meints (ICPP)

10h15-10h30 Introduction into the objectives of the workshop, the agenda and organisational information; Martin Meints (ICPP)

10h30-11h45 Presentation, Günter Karjoth (IBM):

Practicability of protection mechanisms for RFID tags in relationship to their physical capability

Questions, Discussion and Answers:

Various questions concerning the technical abilities of various types of RFIDs in the context of ID documents were answered; a central point was the use of RFID for tickets for the Football World Championship 2006 in Germany. Central aspect of the discussion was that RFID tickets raise important privacy issues. Among them is the question whether the huge processing of personal data which is needed to install such a system is really necessary (principle of proportionality) to achieve the reported goals (i.e. limiting criminal actions by hooligans). Moreover, such a system would augment the risk of profiling and allow interconnection of databases.

More in general, Mr. Karjoth explained that there are multiple privacy concerns connected with the use of RFID which should be dealt with, namely
1. the use of unique identifiers for *all* objects,
2. massive data aggregation,
3. possibility for individual tracking and profiling,
4. stored data to be altered and
5. the availability of scanning RFID tags from a distance (further discussed in the presentation of Mr. Pfitzmann, "id-document specific bombs" and the website www.rftracker.com).

Finally, Mr. Karjoth gave some practical advice to protect oneself against RFID technology (e.g. shield your RIFD readable passport in a Faraday cage by wrapping it in aluminium, use RFID sensor detectors or active jamming (a device which actively broadcasts radio signals to block/disrupt RFID readers)).

A better – infrastructural – solution could be that the manufacturer provides a way to deactivate the RFID tag. In practice, one could think of (non-reversible, password controlled) "kill commands" in shops where RFID protected goods are purchased, in order to obtain post purchase privacy for the customer. This command could take the form

of a device that "kills" the RFID tag, in a similar way as book protections are deactivated in libraries.

An enhanced solution would be the usage of "smart" RFID tags which could be anonymised instead of deactivated.

11h45-12h00 *Coffee break*

12h00-13h00 Invited speaker Markus Nuppeney (German Federal Office for Information Security)

Explanation and Demonstration of the "Golden Reader Tool"

Demonstration:

Using an optical passport reader (used to scan the printed MRZ code) and a contactless smart card reader, Mr. Nuppeney demonstrated how the golden reader tool makes it possible today to access electronic information from *different* kinds of *machine-readable* passports.

Mr. Nuppeney took the opportunity to present the German ILSE project, which aims to obtain interoperability for passports.

Concrete results of this project are the "silver data set", a reference structure for storing different biometric data on a passport which is a very important contribution to the recent ICAO specifications, and the "golden reader tool". This tool is an important step to implement interoperability for passports: it is internationally accepted reference software.

The distance from which the used type of RFID tags is readable is limited; with appropriate readers like the one used for the demonstration 10 cm and almost no movement of the RFID tag is required. With manipulated readers using e.g. more transmitting power, passive detection up to 10 m seem to be reachable. But from this system the chip cannot be activated or the sensor of the reader gets blocked by the power of the transmitter. In these cases the reader cannot receive an answer from the RFID tag.

Questions, Discussion and Answers:

How does the reader react, when two passports are put on him? Mr. Nuppeney demonstrated that in about 50% of the cases the golden reader tool chooses the passport answering first, or reports an error due to overlapping signals.

13h00-14h30 *Lunch*

14h30-15h15 Invited speaker Bernd Martin (Office of the CIO of the Austrian Government)

The Austrian "Bürgerkarte"

Questions, Discussion and Answers:

The main result of the presentation and discussion was that two or more sector-specific personal identifiers ("ssPI") are uniquely connected to the person, but they are not interconnectable between sectors. Basically, a ssPI is just a one way hashed source pin (e.g. health care number of person X or driving licence number of person X), which does not allow the back-calculation of the original source PIN. Consequently, the organisation set up to manage them is an approach to limit the linkage of transactions performed by the same person, which is the main privacy risk discussed with today's PKI and electronic signatures. The "Bürgerkarte" specifically addresses the communication with the various governmental administrations. The solution does not try to achieve full unlinkability: There are ways to link the ssPIs of a person under specific conditions. The disadvantage of this solution is limited interoperability / compatibility on a European level.

It is noteworthy that the Austrian "Bürgerkarte" does not replace the "regular" Austrian ID card and that it exists in different formats (e.g. as a smart card or integrated in a mobile phone).

15h15-16h00 Presentation Lorenz Müller (AXSionics)

Demonstration of the AXS ID-card

Mr. Müller explained that the AXIONICS' goal when they developed the AXS ID-card was to find a way to provide secure authentication, by solving some of the basic problems in IDM, namely by 1. creating a secure link between the person and his/her identity, 2. with simple verification means, that are 3. difficult to forge and 4. which would prevent traceability.

AXIONICS' solution integrates biometric information (fingerprints) in their suggested IDM model.

Questions, Discussion and Answers:

The discussion was focused on the ways how to integrate biometrics in IDM solutions in practice in a secure privacy compliant way. Central topics in the discussion were the problems arising from central storage of *biometric templates* (such as the possibility to retrieve additional personal health information from them, the use (or misuse) of the stored biometric data for other purposes, after the lifetime of the (authenticated) relationship, etc.) and possible strategies to avoid those problems (such as decentralised storage, under exclusive control of the biometric data owner).

Another issue which was raised is the complexity of biometric credentials. Once you start to share these kinds of credentials in identity federation, it creates privacy problems, as it augments the risks of traceability (and identity theft, see the presentation of Mr. Pfitzmann).

The basic idea of the AXS ID-card is to integrate biometrics as part of a 3 factor authentication of a digital credential container, which functions as a token and secure link between the person and the network.

In practice, you authenticate yourself by putting depending on the requested authentication one or more fingers of the requested type an in the right order on the cards sensor. The secret you know (type of finger respectively fingers and their order) allows you to be identified by the device.

A weak point of the current advanced prototype is the quality of the capacitive fingerprint sensor. With a dry finger, there are enrolment and verification problems. The sensor will be improved in the next version of the card and will then be adaptable to the requirements of the user of the card.

The AXS ID-card communicates with the counterparty (the application which requests the authentication) through a visual signal in a web browser. The visual signals (flickering of the screen in four black and white sectors) are registered and interpreted by the sensors on the AXS ID-card.

After the demonstration by Mr. Müller, it was clear that the usage of the card is not as simple as, e.g., the usage of a keyword. This will be taken into account when looking for appropriate markets for this device. Certification of the AXS ID-card following the Common Criteria is planned.

16h00-16h15 *Coffee break*

16h15-17h00 Presentation Andreas Pfitzmann (TUD)

Biometrics – how to put to use and how not at all?

Questions, Discussion and Answers:

Mr. Pfitzmann points out problems with respect to the use of biometrics. Major problems relate to identity theft and profiling, resulting a.o. from the fingerprints industry (fairly easy to counterfeit).

Another big issue is the obvious devaluation of the value of biometrics (leaving someone else's biometrics on the scene of crime).

Furthermore, privacy issues are also at stake, as biometrics generally can contain medical data and (once they are given away) could allow processing without the person's consent.

The only acceptable way – if any – to use biometrics is between the data subject and his/her devices: in this case, there is no devaluation of forensic evidence of biometrics, as they are only used for devices under the exclusive control of the data subject and there are no privacy risks as long as there is no external processing of the data.

However, this use of biometric data does not solve the security problem. In each situation, it should be evaluated how much security is wanted / required and by which means this security level can be achieved.

For instance, it's probably better not to use biometric technology in expensive cars, because of its undesired effects: a thief could 'easily' counter the security measures, by kidnapping the "biometrics owner" or steal his/her biometric data ("cut his finger of").

The result of the discussion was that raw biometric data always contains information, which is not needed for authentication purposes, such as, for instance, medical information. This information is very sensitive from the privacy point of view.

17h00-18h30 Presentation Danny De Cock (KULeuven) and Wim Schreurs (VUB)

Legal and technical aspects of the Belgian ID card

Questions, Discussion and Answers:

The way the card is introduced was discussed. It can be assumed that a citizen to whom this card is issued does not know about the inherent electronic signature and its legally binding character. Apart from this "educational" matter, it appears that there are serious technical and legal concerns:

The concept to deactivate the signature functionality of the card is weak.

Furthermore, the serial numbers of the certificates are based on the national registry number. It is somehow controversial that the usage of the same national registry number is strictly regulated and subject to prior authorisation by a Subcommittee of the Belgian Privacy Commission.

Moreover, the format of this number makes it possible to deduce additional information about the user such as sex, date of birth etc.

Consequently, the problem of linkability of transactions performed by the user via the certificate number appears not to be solved in the first generation of the Belgian eID[1].

[1] It is noteworthy that the ADAPID project (see below) focuses a.o. on this issue and will provide input for the second and third generations of the Belgian eID).

18h30-19h15 Presentation Ian Angell and Dionysios Demetis (LSE)

ID cards: The socio-economic concerns[2]

LSE calculated the total costs of the proposed eID scheme, namely approx. 435 EUR per card (the government' proposal did not include large parts of the needed infrastructure).

Besides the high price tag, there are also severe problems with the proposed eID scheme itself: the proposed technology appears to be immature and very poorly tested.

Mr. Angell explained that even in the test phase, there was a non-negligible group of false positives and false negatives and that there was a very large group of people who were not able to have their biometrics recorded at all. These results would be disastrous on the scale of a population of more than 50 million people.

Questions, Discussion and Answers:

The differences of the registration in Britain compared to other European countries such as Belgium and Germany were discussed.

Planned presentation by Martin Meints (ICPP)

The eCard Strategy of the German Government was moved to the 2nd day of the workshop

19h15-19h30 Discussion and conclusion

[2] Background of this presentation: On 28th of June 2005, the UK government narrowly won the vote on its identity card proposals in the House of Commons. On the previous day, the UK Information Commissioner, Richard Thomas, expressed strong concerns over the government's plans for a biometric national identity card and database.
On 27th of June 2005 (i.e. a few days after the workshop), LSE published its report entitled "The Identity Project: an assessment of the UK Identity Cards Bill and its implications".
The report looks at the potential costs and benefits of the government's proposals and finds that the scheme may be both more expensive and less effective in targeting problems such as terrorism, illegal immigration and identity fraud than the government has claimed.

1.5 Agenda, Minutes and Results, 2nd Day

09h00-10h00 Welcome Martin Meints (ICPP)

Presentation, Martin Meints (ICPP)

Timetable and structure of D3.6 "Study on ID Documents"

The participants agreed in principle on the suggested, preliminary timetable and extended it by a few topics.

Planned table of content:

- Executive Summary
- Introduction
- Basic Technologies for ID Documents
  - Chipcard Technology (such as Operating Systems, Readers etc.) - AXSionics?
  - RFID - IBM, Reading?
  - Electronic Signatures and Biometrics (Summary of D3.2) - ICPP
  - Back-Office Systems (such as Databases, PKI, Golden Reader Tool) - KULeuven, ICPP and others
  - Interoperability / Compatibility - LSE?
  - …
- Legal Grounds in Europe (in co-ordination with WP5, VUB)
  - Overview on the Differences; Link to the Database on Id Law
  - UK / Belgium
  - History and Tradition?
- Leading Concepts, Prototypes and Implementations
  - European Passport
  - Finnish ID Card
  - Austrian "Bürgerkarte"
  - Belgian ID Card - KULeuven
  - German E-Health Card - ICPP
  - …

- ☐ Overview on Concepts, Prototypes and Implementations in EU+ (26 Countries)
  - ■ Table, reference to ADAPID - KULeuven
- ☐ Security and Privacy Aspects - TUD, KULeuven
- ☐ Socio-Economic Aspects - LSE
  - ■ Critical Economic Factors and Suggestions for Implementation
- ☐ Summary, Conclusions and Outlook

Volunteer to do an internal review: Jozef Vyskoc, VAF

To be asked: Bert-Jaap Koops, TILT

10h00-10h30 Presentation, Xavier Huysmans (KULeuven)

Co-Operation with the MODINIS Identity Management project (lot 3) (http://www.egov-goodpractice.org)

Questions, Discussion and Answers:

There appears to be a clear interest to create synergy with MODINIS, at least in the field of the identity management project of MODINIS (as this was the subject of Mr. Huysmans' presentation).

The collaboration could be carried out in practice through attending the MODINIS / FIDIS workshops and/or organising joint workshops) and by having some FIDIS members becoming a part of the MODINIS' working group that analyses case studies and identifies good practices of identity management.

It was noted that the questions with regard to practical FIDIS involvement in the activities of MODINIS should be expressed more concretely and directly addressed to the Work Package leaders. If needed, FIDIS can provide experts for certain areas of knowledge and give answers.

10h30-10h45 Presentation, Claudia Diaz (KULeuven):

Content and Possible Input Provided by ADAPID

This project, funded by the Flemish Government, puts forward a framework for advanced applications (secure, privacy-enhanced) of the eID card in the field of e-Government, e-Health and Trusted Archiving. It started in July 2005.

Central research topics are:

1. Privacy enhancing technologies for the eID,

2. Pseudonyms, unlinkability of unique identifiers, anonymous communication, anonymous credentials,…
3. Biometrics,
4. Trusted modules and
5. Formal Methods.

Possible input from the ADAPID project was integrated in the table of content for D3.6.

10h45-11h00 *Coffee break*

11h00-12h00 Presentation by Martin Meints (ICPP)

The eCard Strategy of the German Government

Mr. Meints presented the status of the 3 German government projects being part of the e-card strategy of the German government.. The first one is in the field of e-health ("Gesundheitskarte"), the second one in the field of employment ("JobCard") and the third one about the implementation of an electronic tax declaration. Detailed information on the planned German eID card was not available at that time.

An advanced prototype of the e-health card contains several kinds of information (from blood group type to allergy data and emergency data), where

1. No medical data is stored elsewhere than on the card and

2. Depending on the requirements to access the data on the card is stored in separate and secured sections of the card.

The current concept of the JobCard raises severe privacy issues, for instance:

1. Possible interconnection of data, due to the central storage (whereas the same data were stored in a decentralised manner before).
2. No clear definition of the purpose of storage and processing of the data (who needs them, when and what for?).
3. Duration and content of the stored data is not sufficiently defined (data minimisation principle is violated).
4. Inappropriately defined organisational and security requirements: vulnerability of the system concept of access to these data may result.

Questions, Discussion and Answers:

The discussion focused on the e-health card, especially ways to store the planned data and to access them in various discussed scenarios such as a prescription or a case of emergency. It was not clear whether any access on data of the card would be logged.

12h00-12h30 Discussion and conclusion of the workshop

2 Conclusions

This workshop had three objectives:

1. To exchange experience about planned or introduced ID documents using new technologies such as electronic signatures, biometrics, and RFID within the FIDIS NoE
2. To get information concerning planned or introduced ID documents from outside the network
3. To organise the content of D3.6 “Study on ID Documents” by discussion of the table of content and co-ordination of the contributions of the partners

Those objectives were achieved as far as it is possible within a single workshop. The invitation of external speakers provided valuable input for the FIDIS NoE, though one concept known to be quite advanced, the Finnish ID card, could not be covered due to the lack of time in preparation. This topic will be further evaluated in the preparation of D3.6 “Study on ID Documents”.

Towards the organisation of the content of D3.6, important progress was made. This includes the identification and co-ordination of contributions to the same topic, such as RFID or technical and privacy aspects. It is expected that the overview of concepts, prototypes and implementations of ID documents will probably be covered largely by the ADAPID project; KULeuven will integrate this input as a cross reference into this deliverable. But a further survey of the FIDIS partners may be necessary.

All relevant partners who are going to contribute to D3.6 with two exceptions due to collision of dates were present with competent personnel at the workshop. The two partners not present kept in contact with the WP3 leader before this workshop and explained if and perhaps what they are willing to contribute so that their proposed contribution could be part of the planning at the second day of the workshop. Further co-ordination will be done within the preparation phase of the deliverable.

We got an especially good feedback concerning the quality of the workshop by the invited speakers. They are willing to provide further material for the preparation of D3.6 and showed a great interest to get the deliverable when published.

The time for questions and discussions was too short. The topic “ID Documents” provides material for at least a two-day workshop, so this concept for the workshop was a compromise. As we shifted one presentation to the second day, we had more time for the discussion on the first day, as this was apparently needed. We will plan more time for questions and discussions in future workshops that have a high potential for questions and discussions.

Annex 1: List of Participants

21st of June 2005:

Name	First Name	Institution
Angell	Ian	LSE
De Cock	Danny	KULeuven
Demetis	Dionisis	LSE
Deng	Mina	KULeuven
Diaz	Claudia	KULeuven
Frehs	Stephan	LSE
Hansen	Marit	ICPP
Huysmans	Xavier	KULeuven
Karjoth	Günter	IBM
Martin	Bernd	Office of the CIO of the Austrian Government; invited speaker
Meints	Martin	ICPP
Müller	Lorenz	AXSionics
Nassary Zadeh	Layla	GUF
Nuppeney	Markus	German Federal Office for Information Security; invited speaker
Pfitzmann	Andreas	TUD
Rannenberg	Kai	GUF
Rossnagel	Heiko	GUF
Royer	Denis	GUF
Sackmann	Stefan	ARU-FR
Schreurs	Wim	VUB
Ulbrich	Martin	JRC
Vyskoc	Jozef	VAF

22nd of June 2005:

Name	First Name	Institution
Angell	Ian	LSE
De Cock	Danny	KULeuven
Demetis	Dionisis	LSE
Deng	Mina	KULeuven
Diaz	Claudia	KULeuven
Hansen	Marit	ICPP
Huysmans	Xavier	KULeuven
Karjoth	Günter	IBM
Meints	Martin	ICPP
Müller	Lorenz	AXSionics
Nassary Zadeh	Layla	GUF
Royer	Denis	GUF
Schreurs	Wim	VUB