FIDIS

Future of Identity in the Information Society

Title:	D8.5: “Report on inter-disciplinary workshops”
Author(s):	Sabine Delaitre, Barbara Daskala (IPTS)
Editor(s):	Ioannis Maghiros (IPTS)
Reviewer(s):	Martin Meints (ICPP) James Backhouse (LSE)
Identifier:	D.8.5
Type:	[Deliverable]
Version:	1.0
Date:	Friday, 21 April 2006
Status:	[final]
Class:	[Public]
File:	fidis-wp8-del8.5. interdisciplinary_workshops.doc

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel (VUB)	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven (KU Leuven R&D)	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)*
1	27/03/2006	Initial release v 0.1 (IPTS)
2	13/04/2006	Review (ICPP – Martin Meints)
3	18/04/2006	Review (LSE – James Backhouse)
4	20/04/2006	Modified version (IPTS)

Table of Contents

Executive summary

FIDIS is a multidisciplinary Network of Excellence and its work is structured into separate research activities. One of these activities is Workpackage 8 (WP8), "Integration of the NoE", that aims at developing interrelations between partners active in different Workpackages by such activities as: organising events where different FIDIS partners may meet, merging subjects from different disciplines, and by raising questions on challenging issues. In this regard, three interdisciplinary, integration workshops were organised during the 2nd FIDIS work plan to address the objectives and main subjects of WP8:

a) Preventing Identity Theft
b) Identity, Emerging Technologies and Trust
c) Identity Challenges in a Mobile World.

The organisation of integration workshops seeks to intensify interaction, foster consensus and develop a common knowledge base in order to generate permanent links between FIDIS partner organisations. In line with these objectives, these integration workshops aim at maximising knowledge sharing and spreading of excellence. To this aim, external (non-FIDIS) experts were also invited to speak at these workshops to contribute their knowledge and expertise on the relevant subjects. As well as being thematically focused, these interdisciplinary workshops sought to converge diverse identity-related subjects, to raise interesting questions and to challenge fundamental notions. The purpose was to identify and bridge gaps in the knowledge base, while promoting Network integration.

This report presents the outcome of all the planned and executed events within the framework of WP8 and as such it describes deliverable 8.5. The three workshops are presented in three chapters and then some conclusions are also drawn. The main aims and results are presented below:

For the first WP8 event / workshop, the target was to bring together partners from WP3 and WP5, i.e. identity-related technologies and de-identification technologies. Hence, the workshop's goal was to identify relevant issues and examine actions and solutions associated with identity theft/fraud. The workshop was organised in cooperation with FIDIS partner Tilburg University who leads WP5. Thus, the central topics of this WP8 event were:

- Technologies to protect / secure data from abuse and
- Processes and methods to counter identity fraud.

An analysis of a working definition for the complex concept of "Identity Theft" from the legal, technological, and social context was the main result of this workshop. Biometrics, RFID and other identity related and emerging technologies were debated as to their potential for curbing identity fraud.

The second WP8 event / workshop aimed at merging issues from WP3, WP4, WP5 and WP7; its main goal being the identification of relevant issues and the examination of actions and solutions associated with emerging identity technologies and trust. The workshop was organised by IPTS WP8 Leader in cooperation with FIDIS partner VIP and the central topics were:

- How to build trust? What processes and methods enable trust?
- Which technologies can provide a trusted framework to deal with identity information?
- What is the role of identity in emerging technologies?

An analysis of the main dimensions of trust and their legal, social and technological components, presented in a table form was the main result of this workshop. Privacy models, anonymising techniques, strong encryption and biometrics were all considered as likely solutions to enhance trust.

The objective of the third WP8 event / workshop was to identify relevant issues and examine actions and solutions associated with identity challenges in a mobile world, merging issues from WP5, WP6, WP7 and WP11. The aim here was to consider identity challenges in mobile communications as well as of individual mobility needs. Thus, the central topics were:

- How does mobility in the information society emerge? In what way are new technologies influencing mobility?
- What is the relationship between identity and mobility? What is the role of the user? How to meet the different requirements of identity in a mobile and non-mobile world?
- What is the impact of mobile services on information society? What are the issues, challenges or opportunities that stem from the issue of mobility?

User requirements when developing mobile applications were extensively debated as were possible Digital Rights Management solutions and international standardisation initiatives for mobile applications in the Academic world. The panel discussions that followed revolved around the emergence of challenges that are being dealt with as well as “dark areas”, namely negative aspects, related to mobile identity.

In this context, through the WP8 workshops, integration and networking of FIDIS partners has been facilitated and promoted, by means of the opportunity to come together, exchange knowledge, information and expertise. It was also possible to develop content integration between the various Workpackages of FIDIS, since the subjects selected for each workshop drew from issues addressed in the various Workpackages. Furthermore, in the context of these workshops, and especially through the discussions and debates, research gaps have been identified for future consideration.

1 Introduction

The fifth deliverable of WP8 "Integration of the NoE", is a series of 3 inter-disciplinary workshops, organised in the context of WP8 from April 2005 onwards. This report summarises the outcome of these workshops. The workshop minutes have been posted on the FIDIS web site shortly after the events took place.

1.1 FIDIS Background

FIDIS objectives are shaping the requirements for the future management of identity in the European Information Society and contributing to the technologies and infrastructures needed. The work of FIDIS is currently structured into 7 research activities:

- "Identity of Identity"
- Profiling
- Interoperability of IDs and ID management systems
- Forensic Implications
- De-Identification
- HighTechID
- Mobility and Identity

As a multidisciplinary and multinational NoE, FIDIS comprises research experience from different countries, each with its own special focus, and integrates European expertise around a common set of activities. Additionally, all relevant stakeholders are addressed to ensure that the requirements are considered at different levels. FIDIS overcomes the extreme fragmentation of research into the future of identity by consolidating and fostering joint research in this area. Research results will be made accessible to European citizens, researchers and in particular to small and medium sized enterprises (SMEs).

1.2 Background on Deliverable 8.5

The objective of WP8 is to generate a set of integrated activities to guarantee effective cooperation within the network. The FIDIS multidisciplinary Network of Excellence contributes to shaping the requirements, definitions and development of the concepts of identity and identity-related technologies. In this framework, WP8 aims at developing interrelations between Workpackages by merging different subjects, raising questions and challenging issues. The following deliverable was elaborated as part of this WP for the 2nd FIDIS work plan:

- D8.5 - Interdisciplinary workshops for the researchers within the network and an overview report on interdisciplinary workshops

This report presents the outcome of all the events planned and completed in this context (Deliverable 8.5). In the first three chapters the minutes of the workshops that were organised within the WP8 framework, are presented; namely:

- Integration Workshop on Preventing Identity Theft - Tilburg, NL, 19th May 2005
- Integration Workshop on Identity, Emerging Technologies and Trust - Biel, CH, 15th September 2005
- Workshop "Identity Challenges in a Mobile World" - Seville, Spain, 24th and 25th November 2005

The organisation of these integration workshops targets the intensification of interactions, the growth of consensus and the development of a common knowledge base aiming at creating permanent links among FIDIS partner organisations. The workshops were organised by the partner IPTS (WP8 leader) in cooperation with other partners so as to maximise benefits without over-burdening the participants.

The selection of the subjects and issues for each workshop was driven by the desire to cover areas not previously addressed by the other FIDIS Workpackages, as well as to examine new areas for future research. It was also important to build on existing knowledge and expertise, that is, where possible, to use as input or combine the results of the work being done in the other Workpackages. In addition, external experts were invited where their expertise was seen to contribute to the general debate.

In the last section, some concluding remarks are presented in relation to methodology and substantive achievements, and the overall organisation of the workshops.

2 Integration Workshop on Preventing Identity Theft

2.1 Introduction

The organisation of integration workshops seeks to intensify interaction, foster consensus and develop a common knowledge base in order to generate permanent links between FIDIS partner organisations. In line with the first event's objectives, this second integration workshop aims at maximising knowledge sharing and spreading of excellence. Beyond being thematically focused, these interdisciplinary workshops aim at aiding the fusion of diverse identity-related subjects, at raising interesting questions and at challenging the main issues. In this case, the objective of the workshop was to help integrate the diverse visions on identity theft and identity fraud.

For the second WP8 event, we sought to build bridges between subjects from WP3 and WP5, i.e. Identity-related technologies and ID-theft, Privacy and Security. Hence, the workshop goal was to identify relevant issues and examine actions and solutions associated with identity theft/fraud. The workshop was organised in cooperation with FIDIS partner Tilburg University which leads the WP5. Thus, the central topics of this second WP8 event were:

- Technologies to protect / secure data from abuse and
- Processes and methods to counter identity fraud.

After a short welcome by B.J. Koop of the host organisation (Tilburg University), Ioannis Maghiros (IPTS), WP8 Joint Action Leader, introduced the workshop, described the workshop approach, its objectives and the planned sessions. He explained that the format of this workshop included presentations on specific subjects as well as brief introductions to points that needed to be discussed at length. He underlined the need for active participation that would lead to the exchange of information and knowledge necessary to achieve real integration. He also thanked the guest speaker, Stephan Engberg from Open Business Innovation, for having accepted the invitation to contribute and present on "Counter to Identity theft, privacy solutions". He finally wished all a fruitful and productive workshop.

Brief descriptions of the presentations and analysis of the salient points are detailed below, as well as the main points of both discussion sessions. The list of participants and the agenda of the meeting is also enclosed. All presentations are on the FIDIS web site.

2.2 Summary of presentations

Zeno Geradts (NFI) made a presentation on biometric techniques and their impact on identity fraud. This presentation introduced different biometric techniques such as iris, retina, voice, hand and fingerprint recognition. It provided evidence on how to spoof them e.g. picture of iris with a hole, use of gelatine leaves for performing fake fingerprint, picture of the hand, etc. Afterwards, he described the compatibility features of each. Compatibility feature refers to user friendliness but it does not include accuracy results. So face recognition seems the more user friendly technique, then fingerprint and iris. Retina appears as the worst technique in respect of ease of use.

(Invited session)

Stephan Engberg (OBI) gave a presentation on how to counter to identity theft, and suggested some privacy solutions. The main idea of his presentation was how to empower the individual to take control of the process of identity creation and use as (s)he is the only one who stands to gain or lose from its mismanagement. More than a privacy enhancing solution, he advocated that what is required is a real security solution. He proposed that context-adaptable recognition enriched with appropriate accountability features is what we ought to be looking for.

Related to the presentation on biometrics, he recommended that:

- Biometrics be used as a more secure and more convenient alternative to passwords for device-based local authentication. Biometrics could be useful only if biometrics are to be used as a PIN code. He suggested that biometrics are not a secure solution for identification purposes but suitable for local authentication only. He pinpointed the main problem with biometrics as their lack of revocability. He was convinced that regarding global identification, biometrics would generate more risks than they may resolve.

He initiated his presentation on privacy solutions to counter identity fraud by describing an RFID example case. He was convinced that in order to enhance security and privacy in the digital world, personal identification should be done through devices. ("bridging information"). He proposed a RFID-based solution only possible if a more sophisticated tag (more complex than today's standard passive tags) were used. He underlined the fact that RFID use was not suitable for strong authentication and that it should be programmed not to respond to a challenge with a password as this way it was very easy to trick the system. Overall, he mentioned the following security problems when using ordinary passive RFID tags:

a. counterfeiting
b. eavesdropping
c. traffic analysis
d. denial of service
e. loss of privacy
f. corporate espionage

From this solution approach, some interesting points enhancing privacy are worth underlining:

- built-in authentication (device-based)
- non-targetable device (one that uses non-predictive identifiers)
- zero-knowledge systems
- context recognition before revealing context
- user's ability to generate predictive ID (mobile IPv6 home address-based)
- instant revocability
- anti-phishing
- empowerment + context → trust model based on risk prevention
- allow military-grade encryption

For further details: www.obivision.com/papers/PST2004_RFID_ed.pdf

2.3 Discussion 1: definitions identity theft - identity fraud

As a result of the diverse definitions used in the earlier-made presentation, IM insisted on the need of harmonization on definitions; only a common definition will enable an appropriate collection of information.

The discussion first focused on identity theft and its terminology. The word theft was used but it did not represent accurately the notion. From this discussion, some concepts arose as significant elements to be taken into account to define Identity theft: INTENT, CONSENT, DAMAGE and VICTIM's point of view. Damage is a concept that may be legally defined while intent and consent require more debate in a legal context. It was possible to limit the debate by not embarking on a legal definition of the term yet.

In order to help the reasoning, different steps structuring "identity theft" have been suggested:

4 steps (TILT)	2 steps (ICPP)	4 steps (Karlstads Univ.)	2 steps (VIP)
FISHING MISSAPPROPRIATION MISUSE CRIMINAL ACTION	ID TAKEOVER (assuming an ID) ID MISUSE	COLLECTION AGGREGATION ID CREATION CRIMINAL ACTION	PROFILING MALICIOUS INTENT

Some other elements have been identified for specifying/qualifying the first ones:

- actual or potential damage,
- risk of damage because of the data collection,
- consent implies the acceptance of the risk.

Other elements emerge but they are regarded as useful for the categorisation of different acts as identity theft or not or identity fraud or not. The list of these elements is the following:

- civil or criminal law,
- undesirable/illegal use,
- liability (protection),
- identity creation (based on partial identities), and roles (partial identities).

Finally, the starting point of ID theft is always the identity transformation of an existing identity, while ID fraud can also be committed by abusing non-existing identities. The second point to consider is the intent (whether malicious or not) of the transformation which is a term that is both very difficult to define legally and also cannot be proven but only after someone has been victimised. The third point to consider relates to the consent for the data collection that may eventually lead to ID theft; in case of no consent; we are faced with identity theft. The fourth one concerns the use of identity information. If it leads to a criminal act then we are faced with Identity fraud.

Attempt at a definition:

One definition

Identity theft is the act of obtaining someone's identity information without the person's knowledge and in order to commit criminal activities

After discussion

Identity "theft" is the act of obtaining someone's identity information without the person's consent and with malicious intent.

Since the word theft does not represent the actual action the following words have been proposed to replace it: sequestration, seizure, misappropriation, hijacking, abduction, deceitful takeover, capture!

Use of false identity is punishable in most EU Member States although in a distinctly unharmonised manner. Important to remember that identity fraud can happen without identity theft happening; in this case only a legal definition will do. In case identity theft happens (as in phishing – which is already illegal art.6b of the Data Protection Directive) specific ID laws should exist to punish it as it represents a risk.

2.4 Discussion 2: debate session

This session was structured as follows: a short presentation of one partner in order to transmit one message and to kick-start the discussion.

Bernhard Anrig (VIP) dealt with 2-ways and 2-channels for authentication.

The presentation focused on the different basic concepts for authentication, i.e. 1-way authentication, 2-channel/2-factor and 2-way authentication. 2-channel and/or 2-factor authentication is best used in a local environment as a replacement/enhancement to passwords. It can fight off Trojan type of attacks but is considered not as secure solution in global authentication problems. 2-way authentication is in theory even more secure procedure as it implies the establishment of two certificates; one to the sender from the recipient and another one to the recipient from the sender. This procedure can be made even stronger if zero-knowledge authentication procedures are added. However, it seems that even such an extremely secure procedure will not in practice solve our identity theft problems. Man-in-the-middle attacks cannot be avoided when using this method and individuals will always have the problem of not knowing which certificate (from which site) to trust.

Martin Meints (ICPP) presented draft guidelines on how the current authentication technologies should be used to enhance security. His objective is to develop a list of criteria or guidelines that technologies should meet in order to limit the likelihood of identity fraud. He outlined the need for such criteria with two examples where authentication procedures (1) are not secure enough, thus facilitating a considerable amount of fraud and (2) "over-authenticating" users by requesting information that is not needed for that specific authentication procedure. The assumption is that properly used authentication systems will

increase security while at the same time reducing the risk for identity theft through reduced use of sensitive authentication information. He detailed sets of guidelines regarding authentication for the different social and functional systems corresponding to roles and personal needs that should meet at least two criteria (level of security and diffusion of the service). The connection to identity theft is that although we will not be able to defeat it we might at least limit it through safer authentication procedures.

Mireille Hildebrandt (VUB) presented some elements about the risks of a networked AmI environment for de-identification. She shortly described the three possible ways used for the misrepresentation: biometrics, attributes or historical footprint (HF). It seems more difficult to misrepresent someone by using HF than by other modes. However, HF can engender profiling and create false positive. The challenge then is to use un-linkable data sources to prevent identity fraud and to allow linking as a means of facilitating profiling.

During the first day workshop, Andrew Wallwork and Stephen Freh (LSE) presented on how interoperability (IOP) of identities can influence the battle against identity theft. On the one hand it is clear that in this new world in which identities are replaced by tokens IOP will facilitate faster and easier access to information. On the other to do that we are considering transferring the liability of identification to the (most likely weakest link) human element (no way to take out the human from identification). In the same way IOP will help combat identity fraud as it will also facilitate greater opportunism in committing it. Overall it is the impression of the presenting partner that more technical IOP and less procedural may be an appropriate mix to fight for less identity fraud.

Overall, the presentations dealt with how to make more secure transactions possible. From the discussion, the un-linkability topic was raised and its necessity was underlined; indeed the linkability of data makes the consequences of identity theft worse and makes possible the surveillance society and increases fear. Stephan highlighted the need to distinguish the different spheres (private, professional, social) and the need to identify (and implement) a correct balance between control and decision in the digital world. And a solution is suggested: the establishment of a temporary linkability between two contexts.

Another topic discussed (introduced by B.-J. Koops) was about the victim's identity recovery and how to help the victim. Consumer organisations should be made responsible for helping victims retrieve their true identities. Legislation that defines liability issues in case fraud has business implications but the consumer should not be involved.

2.5 Actions

After this second successful WP8 integration workshop, Ioannis again underlined the importance to define a way to capitalise on the information produced and exchanged during these meetings, other than just disseminating the minutes and possibly gathering any feedback.

Some of the results and open issues of this workshop were taken up by the FIDIS partners and worked out in contributions to the additional Deliverable "D5.2a Identity Theft, Identity Fraud". This was especially true for security and privacy aspects of authentication and the value of such measures to prevent identity theft.

The next WP8 workshop aiming at combining topics from different Workpackages will be on "Identity emerging technologies and Trust". IPTS in collaboration with VIP will prepare and present this third WP8 workshop which is planned for September 2005.

List of participants

▪ Bernhard Anrig, VIP ▪ Emmanuel Benoist, VIP ▪ Stephan Engberg, OBI ▪ Martin Meints, ICPP ▪ Zeno Geralts, NFI ▪ Bert-Jaap Koops, TILT ▪ Ronald Leenes, TILT ▪ Ioannis Maghiros, IPTS ▪ Sabine Delaitre, IPTS	▪ Mireille Hildebrandt, VUB ▪ Wim Schreurs, VUB ▪ Michiel Verlinden, VUB ▪ Jozef Vyskoc, VaF ▪ Michaël Vanfleteren, ICRI ▪ Mark Gasson, Reading ▪ Iain Goodhew, Reading ▪ Ben Hutt, Reading

3 Integration Workshop on Identity, Emerging Technologies and Trust

3.1 Introduction

In line with the first event's objectives, this second integration workshop, in the frame of WP8, aims at the integration of the diverse visions on identity emerging technologies and trust.

3.2 Second Integration Workshop

For the second WP8 event, which was hosted in Biel, Switzerland, by FIDIS partner VIP, we targeted building bridges between subjects from WP3, WP4, WP5 and WP7. Hence, the workshop goal was to identify relevant issues and examine actions and solutions associated with identity emerging technologies and trust. The workshop was organised by IPTS WP8 Leader) in cooperation with FIDIS partner VIP. Thus, the central topics were:

- How to build trust? What processes and methods enable trust?
- Which technologies can provide a trusted framework to deal with identity information? What is the role of identity emerging technologies?

After a short "welcome" by David-Olivier Jaquet-Chiffelle of the hosting organisation (VIP) and the director Christine Beerli of the "School of Engineering and Information Technology – HTI", Sabine Delaitre (IPTS) also welcomed participants, described the workshop approach, its objectives and the planned sessions. She explained that the format of this workshop includes presentations on specific subjects as well as a session with invited speakers. She underlined the need to foster the exchange of information necessary to achieve the integration effect. She finally wished all a fruitful and productive workshop.

The document that follows contains brief descriptions of the presentations and analysis of the salient points. The list of participants and the agenda of the meeting is also enclosed. These brief minutes and all presentations will be on the FIDIS web site.

3.3 Summary of presentations

Martin Meints (ICPP) gave a presentation on "Trust - The Role of Privacy Commissioners" aiming at defining trust in IT systems, detailing the tasks of trusted parties in technology design and their role in operational procedures. ICPP is the data protection authority for the 'Schleswig-Holstein' region of Germany. The mission of ICPP as a trusted party is to guarantee privacy and data security, and to defend the citizens' privacy rights. Thus, their main tasks are the monitoring of the use of personal data (control visits, review of documentation and implementation of IT systems), the processing of the submitted complaints and the offer of consulting services.

From the ICPP's point of view, trust needs safety, security and privacy and can be supported by the use of certificates and seals for instance. The ICPP's privacy seal program was presented through which some 30 seals have been delivered until today. ICPP has to control the compliance of a product that bears an ICPP seal in terms of its protection of privacy and is

also responsible for the privacy protection offered by the public sector (ICPP audits for procedures in the public sector within the German framework).

Remark: MM raised the question of whether a European seal should exist.

Marek Kompost (Masaryk University) provided a short presentation from his first research work on how to model privacy with respect to contextual information. The main goal of his approach is to consider some options for privacy quantification, such as providing a model facilitating the inclusion of as many aspects of user interaction as possible and this, with a view to assessing the possibility to do semi-automatic evaluation of privacy.

He defined privacy by the integration of 4 elements, namely anonymity, pseudonymity, unobservability and unlinkability with the following definitions:

- anonymity: anonymous use
- pseudonymity: pseudonymous use
- unlinkability: several uses which may not be linked
- unobservability: not knowing that a service is used

In order to identify and define the context information, he introduced the Freiburg Privacy Diamond Model in which contextual information encompasses information related to device and location. The proposal from his work is the PATS (Privacy Across The Street) graph. Through this graph the prospective attacker's knowledge is modelled, since the attacker's knowledge stems from the available contextual information. The expected outcome of this graph is the likelihood of "which service is used by which user?"

Future work planned will focus on the further development of this idea and most likely will focus on analysing for example: how PATS can be used to improve privacy in an investigated system? Or what kind of relation to reputation systems exists?

E. Benoist and B Anrig (VIP)

This presentation on "Anonymisation as a part of trust scheme" is about enhancing trust through anonymity. The main topic was trust and how to achieve it? First of all, the necessity of trust was introduced. Anonymisation consists in providing a process in order to disable – to hide – the link between the data and the physical person. This process would thus render impossible identifying a physical person from the corresponding data knowledge (one way process). The proposed scheme is an encrypted "fingerprint"; here, a fingerprint of a person is represented by the following set of information "name + first name + sex + date of birth".

The anonymisation process is composed of 3 steps: generation of the fingerprint (collection of the information set), transmission of fingerprint (to central office) and generation of a uniform fingerprint (encryption process). Anonymisation is only one part of trust scheme, the need to provide proof of trust and to use standards and certifications was raised.

Remark: As it is possible to access, the set of information is not secret (i.e. it would be possible to gather this information from an unprotected ID card for instance).

Danny De Cock (K.U.Leuven) provided a presentation composed of two parts: "Unique Person Identifiers" and "Belgian eID Card Trust Model".

Hence, the first part was about "Unique Identifiers" and, more precisely, the design of a system that provides unique identifiers, e.g., applied in the healthcare context (medical doctors, pharmacists, labs, hospitals), but distinct identifiers in privacy-sensitive sectors (insurance companies, statistical analysts). The schematic overview and the requirements of such a system were presented, such as that the distinct identifiers in the privacy-sensitive sectors should not be linkable to the person's identity without approval and cooperation of a trusted party. The UPI (Unique Person Identifier) calculation algorithm is typically based on a MAC algorithm, e.g., based on the well known encryption algorithms 3DES or AES.

The second part of the presentation was entitled "Belgian eID Card Trust Model" (copies of the slides were distributed). At first a quick overview of the topic was presented focusing on the different aspects of use, such as authentication, creation of digital signatures and others with the eID Card containing administrative data, including photo, address, cardholder identity, etc. Mr. De Cock stressed that the content of the Belgian eID cards can only be managed by the government. It was pointed out however that currently, all the files stored in an eID card (certificates and citizen data) are available to be read by anybody who can access the eID card's chip. The speaker continued on to mention that the issuing process of an eID card depends on the physical authentication of the person at the municipality. Once the eID card has been issued to the citizen, the citizen can authenticate himself towards third parties using his eID card. The certificate hierarchy was presented (five certificates are stored in the eID Card: the certificate of the Belgium Root CA, a Government Certificate, the Citizen CA, and two citizen certificates). Using these certificates, the citizen is able to validate the trustworthiness of a complete certificate chain, e.g., obtained from a web server or an email sender. The two certificates issued to the citizen can be used to authenticate the citizen and to produce a digital signature legally equivalent to a handwritten signature. The Belgian eID card does not support encryption keys and thus does not require any encryption certificate.

Trust aspects:

- eID card trust model relies on delegation
  - CA delegates responsibility to government
  - Government delegates responsibility to citizen
  - Application default configuration
- Trust model mostly relies on
  - Reputation of the manufacturers
  - Good behaviour of citizen
  - Correct behaviour of the application software
  -

Ronald Leenes (TILT): "Trust in PRIME"

Mr. Leenes provided a presentation that summarised the 'Trust in PRIME' workshops held during the PRIME general meeting in Bristol (7 and 8 of September). The PRIME project aims at creating technical solutions for Privacy and Identity Management. These solutions will be implemented in different EU countries with different social and cultural standards. In designing user-centred IDM applications, trust is an important issue, both from a technical

perspective as well as from a social, legal and economic perspective (SLE). The technical Workpackages deal with establishing trusted platforms, secure communication, encryption etc. The average user will likely not understand these technical measures that aim to protect her privacy.

Hence, they have to trust that the technology performs as advertised. An observation in trust literature is that people trust people, but not technology. This is where the SLE Workpackages join in. This aims at determining what triggers distrust in people and how trust can be established and maintained in PRIME technologies. The Trust in PRIME workshops aimed at creating a common understanding of trust issues in PRIME and promoting collaboration between technical and non-technical researchers.

Mr. Leenes gave a brief overview of the material presented in the PRIME workshops. He listed a number of factors establishing trust in the off-line world and in the on-line world and then focused on the on-line world describing trust negotiation (credentials, privacy seals and reputation data).

In addition, the traditional market literature and the reputation-based trust (composed of 3 layers: companies, users and Trusted Third Parties) were described and the principles and the sources of trust (i.e. cognition-based trust, affect-based trust) were presented. However, in a remark on negative reputation, the answer was that the system should be carefully designed so that people won't try to misuse the reputation mechanism. Some more slides from the PRIME general meeting were presented showing how to make people feel confident to use technologies in which their privacy is protected by PRIME technologies. RL described the relations between the trust concepts (informal, formal, individual, collective, social, cultural, etc.) and presented a graph showing the users perception on privacy concerns and trust in different countries.

TRUST in PRIME

- trust negotiation
  - credentials
  - privacy seals
  - reputation data
- compliance checking/assurance
- obligation management
- platform trust management
- trusted user interface

Invited Expert session

Emilio Mordini (Centre for Science, Society and Citizenship, Roma, Italy) gave a presentation on ethical issues in the use of biometrics. He is the coordinator of the BITE project (Biometric Identification Technology Ethics) project. www.biteproject.org

The main topic of this presentation is the use of biometrics as individual identifier. After an introduction on biometrics, EM gave an overview on biometric technologies, including well-known ones (e.g. face or fingerprint) and less prominent ones (e.g. hand vein or ear pattern recognition) which are however used commercially (Bank of Japan, NOKIA mobile phones). Afterwards, he spoke about policy implications and raised some issues, such as problem of privacy protection, the likelihood of 'function creep', the foreseen vulnerabilities of some groups of people (disabled, drug abusers, population on the move), stigmatisation and the "living test".

He introduced the use of biometrics as a step in the revolution of identity and explained the creation of legible population: a people open to the scrutiny of the officialdom. The speaker presented a slide in order to introduce the idea that identities subsequently are no longer guaranteed by Nation States.

Finally, he provided an overview of the BITE project and its corresponding work plan and informed the participants on future events organised by BITE, such as:

- 15-16 December Brussels, Science and Society workshop organized by the EC.
- BITE final conference – September 2006.

Biometrics and Trust

In pursuit of the Lisbon strategy to become an inclusive, dynamic, competitive and secure knowledge-based society, the European Union needs to provide its citizens and consumers with a 'trusted' online environment. Identification systems are key interfaces between the real world and the digital world, though often, they are invisible to users. Biometric technologies provide a strong mechanism for authentication and therefore can promote the development of a 'trusted' Information Society.

The potential to protect personal data (privacy) as well as to foster security are two main contributions of the technologies enabling trust. Biometrics can be regarded as such a technology. Indeed, a key feature of biometrics is that they have the potential to enhance privacy. This is because biometrics, if appropriately used, can establish identity without connecting this identity to other data sets, such as social security number, driver's license etc. Also, in verification mode biometric systems are able to authenticate a person's access rights without revealing his identity. Moreover, since we carry all our biometrics with us at all times, it is easier to use multiple biometrics to compartmentalise, and therefore further protect our personal information – we might not be able to remember ten secret codes, but we are able to provide ten different biometric samples to separately access ten different systems.

Moreover, one of the main reasons for introducing biometrics is to increase security and the sense of security. Although increased efficiency in law enforcement does not directly improve security, it can be argued that the use of biometrics acts as a deterrent to criminal, illegal or anti-social activities. In this respect, overblown claims about the performance of biometrics may actually prove helpful.

On the next day the participants were introduced to practical examples of identity-related technologies, especially wireless communication and profiling technologies.

3.4 Analytical part

What is trust? Which technologies, components are required to provide trust?

Out of the different presentations, the concept of trust has been defined in many different ways. However, some common knowledge may be extracted in order to draw up some common characteristics/facets of the trust concept. The trust notion involves several aspects; it is not only the result of a technological solution. Indeed, we have to take into account other aspects, such as social, cultural or legal in order to establish and maintain trust. Moreover, trust presents cognitive aspects; indeed, trust mainly is based on experience and reputation and is related to risk perception. Users need proof of trust.

The dimensions of trust are: security, safety, reliability and transparency

Regarding trust, protection of privacy is one transversal dimension with a strong technological part.

In the on-line world, trust is related to credentials, privacy seals and reputation data.

Some challenges to enable trust:

- the use of the strictly necessary data for authentication (Which data has to be stored? What is the role of standards?)
- the need for transparency (relationship between the companies and users)
- to be able to protect personal data (the role of Privacy Enhancing Technologies (PETs)) and defend the user in case of problems (How to put in place efficient Trusted Third Parties (TTPs) and in which legal framework?)
- to make user and personal data unlinkable. (the role of encryption technologies, e.g. AES, IDEA, 3DES)
- to provide clear guarantees (How to define clear responsibilities?)

Out of this analysis the following table is proposed to help in the drawing of conclusions on the challenge of ‘How to enhance trust’

First draft TABLE of definition of trust concept and of its different facets:

TRUST		
Challenge	Facet	Components or technologies involved
Use of strictly necessary data	Technical, structure of the memory	Segregated storage
	Ethical	Standards
Transparency	Social and legal	
Protection of personal data	Technological	PET (e.g. biometrics)
	Structural, model	TTP
Defend user (advocate)	Legal	
Prevent linkability	Technological	Encryption technologies
Responsibilities (one main component of transparency)	Legal, contractual (Economic)	Guarantee

3.5 Actions

Parts of the issues addressed in this workshop will lead to contributions in future FIDIS Deliverables. This includes the issue of trust in eIDs in D3.6 “Study on ID Documents” and trust and biometrics in two planned biometrics related deliverables in the third FIDIS Workplan.

The next WP8 workshop aiming at combining topics from different Workpackages will be on “Identity Challenges in a Mobile World”. IPTS will prepare and present this next WP8 workshop which is planned for end November 2005 in Seville.

List of participants

- Denis Royer, JWG
- David-Olivier Jaquet-Chiffelle, VIP
- Bernhard Anrig, VIP
- Emmanuel Benoist, VIP
- Claude Fuhrer, VIP
- Emilio Mordini, Centre for Science, Society and Citizenship, Roma, Italy
- Martin Meints, ICPP
- Ronald Leenes, TILT
- Sabine Delaitre, IPTS
- Wim Schreurs, VUB
- Vasiliki Andronikou, NTUA
- Jozef Vyskoc, VaF
- Mark Gasson, Reading
- Marek Kumpost, Masaryk University
- Danny de Cock, KULeuven
- Ammar Alkassar, Sirrix
- Dionisis Demetis, LSE
- Lorenz Müller, Axionics
- Marc Sommer, Axionics
- Stefan Gempeler, Axionics

4 Integration Workshop on Identity Challenges in a Mobile World

4.1 Introduction

In line with the first event's objectives and within the frame of WP8, this third integration workshop, aims at integrating the diverse visions on **identity challenges in a mobile world**.

4.2 Third Integration Workshop

For the third WP8 event, which was organised by IPTS (WP8 Leader) and hosted in Seville, Spain, building bridges between issues from WP5, WP6, WP7 and WP11 were targeted. Hence, the workshop goal was to identify relevant issues and examine actions and solutions associated with identity challenges in a mobile world. Thus, the central topics were:

- How does mobility in the information society emerge? In what way are new technologies influencing mobility?
- What is the relationship between identity and mobility? What is the role of the user? How to achieve the different requirements?
- What is the impact of mobile services on information society? Which are the issues, challenges or opportunities stemming from mobility?

After a brief "welcome" by Ioannis Maghiros (IPTS) who chaired the workshop, Sabine Delaitre (IPTS) also welcomed participants, introduced the main topics and described the workshop approach, its objectives and the planned sessions. She explained how the presentations (by FIDIS members as well as by invited speakers) and panel-discussions cover the main topics highlighted in her introduction. She underlined the need to foster the exchange of information necessary to achieve the integration effect. She finally wished all a fruitful and productive workshop.

The document that follows contains brief descriptions of the presentations as well as of the panel discussions and an analysis of the salient points. The list of participants and the agenda of the meeting is also enclosed. These minutes and all presentations are now on the FIDIS web site.

4.3 Summary of presentations

4.3.1 Session 1: New mobile applications and user concerns

Silvia Elaluf-Calderwood (LSE) presented her view on "Identity concerns for the mobile user" and more precisely on the user identity in the mobile working environment. She briefly presented technical capabilities of mobile devices and their relation to different types of mobility; she identified micro, local and remote mobility requirements and defined local and remote types in the context of working activity. In addition, she underlined that the borders between private space and public space are more and more blurred mostly because of user production and consumption of mobile content. The ubiquitous character of mobility, the notion of trust as a bridge between the mobile individual and mobile usage, and the extension

of physical space by virtual space are likely the most relevant trends of mobility in the Information Society. According to her presentation, identity challenges are mainly related to issues of control, data protection and a privacy framework, thus the need to establish a legal framework to protect individuals was stressed; an example of location-based services and what actor has access to what data made the point.

In addition, Mrs. Elaluf-Calderwood introduced the following very important points:

- Some changes of individual behaviour may be regarded as an impact of mobility on the information society; in particular the fact that mobile means to facilitate the publishing of private information (e.g. by blogging while mobile) without the user being fully aware of the possible consequences.
- From a legal perspective on mobiles services, it was underlined that issues related to liability and responsibility concerning data storage, type of data (text, voice, etc.) and storage duration ought to be developed.

.

Martin Meints (ICPP) gave a presentation on "Security aspects of Mobile solutions: lessons learnt from an application for the police of the Federal Land of Hessen" aiming at describing the current solution used by law enforcement staff and detailing the requirements in order to put in place a secure mobile solution. A case study was presented which examines the current security requirements, the different mobile devices, the mobile user tasks and in general the "mobile computing solution". Specific security requirements of the mobile solution include the stabilisation of the network connection, strong authentication, encryption of the network transfer and stored data and secure firewall concept. Mr. Meints underlined the need for reliability and integrity of the data sources, the efficiency of the fallback procedures, the security of stored data. Consequences of, the loss of connection and the physical limitations of the mobile devices were summarised.

The discussion that followed, focused on the difference when considering mobile identity requirements compared to those in wired networks. This is mainly the (in)security of the (changing) location of use of the mobile device. Identity concerns raised during the presentation relate mainly IT security which leads to solutions involving: (i) more network access security for the mobile devices (both for (re)-connecting/(re)-authenticating them seamlessly and for blocking them to/from the network); (ii) proper encryption techniques to guarantee the data during transmission and storage; and (iii) adequate fallback procedures over and above standard market solutions. Other concepts that differentiate mobile user requirements relate to: (a) general restrictions on power consumption and for data input and visualisation due to the small size imposed on mobile devices; (b) the storing of confidential data on the mobile devices which could more easily be compromised; (c) the fact that many devices (especially mobile phones and PDAs) support single user operating system only.

4.3.2 Session 2: Economic Aspects of Mobile solutions and mobile DRM

Invited speaker, Antoñio Maña (University of Malaga) gave a presentation on "Identity and Authorisation for Digital Rights Management (DRM) Applications". AM started with the definition of the DRM concept -as in Management of Digital Rights vs. Digital Management of Rights- and highlighted the need for appropriate enforcement rather than management of digital rights. The speaker identified different categories of existing rights, however noted that these constitute mainly the content owner's rights, whereas there is lack of reflection on users' rights. According to the presentation, the problems in DRM have different aspects, namely social, economic, legal and regulatory and technological aspects. Especially, DRM seems to be a technically hard problem, in the sense of expressing, computing, linking, managing, tracing back, enforcing rights, protecting content and at the same time supporting interoperability, providing flexible models, concealing rights, etc. Mr. Maña raised a point as to the necessity of handling client privacy more as rights enforcement, in this way broadening the DRM scope, as well. With regards to mobile DRM, he identified specific characteristics of the mobile technology and also some challenges that are intrinsic to mobile DRM, such as platform diversity, the user need to keep the purchased rights, as well as the fact that rights and contents are sometimes not on the same device. According to his presentation, mobile devices demonstrate strong technical advantages for the development of DRM solutions; there is more control since it is a personal device and there exist mechanisms to protect sensitive data (IMEI, SIM, USIM + crypto-processor[1]). However, a major problem with mobile devices is the need to backup and restore rights when there is a change of device for a single user.

He also stressed the difference between the terms identity and identification, the former being a more vague concept than the latter, and moved on to the definition of digital identity. Trust here is identified as the ultimate goal, be it reputation-based or certification-based, achieved by identity-based systems and attribute-based systems, respectively. He also noted that in a mobile and a more heterogeneous world, identification is harder, privacy becomes more important and more socioeconomic, legal and technological issues arise. In this context, trusted computing is often offered as a solution in providing this much sought-for trust, which has many advantages, but on the other hand presents certain serious disadvantages as well. As a possible solution, he proposed redefining of DRM, widening its concept and make it target all digital assets. In this case identity will be complimented by associated attribute (rights) attestation; in other words gain trust by limiting the specific purpose for which trust is needed. In mobile terms this may lead from a SIM-centric solution to an enforcing rights solution.

Denis Royer (JWG) in his presentation entitled "Identity Challenges in a mobile world" focused mainly on the economic aspects / dimensions of a "mobile world". First of all, Mr. Royer defined digital identity (individual token & a set of properties) and mobile identity (temporary token & properties related to location and context), and presented four basic domains / aspects of the mobile world, which are very interdependent. In his presentation, the speaker focused mainly on one of these dimensions: The economic.

From his point of view, the economic aspect involves issues such as the diffusion of innovations, the technology acceptance model and the price of convenience. Mr Royer also

[1] Mobile phone security authentication protocols

detailed currently operating business models, such as those covering SMS or ring-tone sales and also others that cover access to networks/communication, content provision and LBS, and future applications, such as mobile signatures, Data Broadcasting/VoIP, Rich Media Content, TV & Interactive applications. The speaker then moved on to what happens in the market regarding qualified signatures. He highlighted a challenge of SIM signature, especially regarding the issue of ownership of the smart card, for which a solution may be found in Certification on Demand. However, profitability is an important factor in the adoption of such a scheme, in the sense that mobile operators and Certificate Authorities (CAs) will only offer signature-capable SIM cards if a positive return on the investment (ROI) can be expected and forecast profitability levels are satisfactory.

The focus of this presentation was mainly on economic solutions / innovations towards protecting and safeguarding mobile identity, however, there was also discussion on the challenges that are going to be raised as to the acceptance of solutions in the market place.

4.3.3 Session 3: Identity technologies for a mobile Europe

Invited speaker, Diego Lopez (RedIRIS) with his presentation on "Identity Management with a European Academic Style" provided us with an overview of various identity technologies and policies used to solve authentication and access control challenges in the European Academic Networks Environment. Mr. Lopez stressed that a basic aim is to allow users to establish their digital identity and rights in the European research and academic networks, an environment which is highly heterogeneous, in terms of infrastructure, protocols and technologies used. To this end, a series of initial services (such as those researched in the project Education Roaming - EDUROAM), technologies and policies have been developed and are used throughout the European Academic Networks. GEANT Authorisation Infrastructure for the research and education community - eduGAIN is the project that allows federated access to services over and above the services provided by all GEANT members. In this project, there exist technologies to allow checking of access rights and syntax and semantics of attributed rights. TACAR [TERENA (Trans European Research and Education Networking Association) Academic CA Repository] is a PKI-based solution within the global academic and research community, attempting to simplify maintenance procedures. Another interesting proposed technology, NAS-SAML, is currently under discussion, aiming at simplifying network and application access with a Single Sign-On solution, and at the same time fulfilling identity management requirements. As regards policies, there is the Cotswolds group initiative, establishing a framework for further international collaboration of AA systems, as well as helping other countries to establish similar large-scale systems. Finally, another policy initiative, the TF-EMC2 (TERENA Task Force on Middleware Coordination and Collaboration), is focused on Identity Management and targets potential users and adopter communities (libraries, e-Learning, healthcare-related activities, etc.), disseminating results both within the EC, the bodies within the European Union, as well as in commercial companies and forums.

Mobility of researchers is a necessity in the academic world. The creation of virtual institutes where there is full collaboration while not sharing the same physical location is highly appreciated. The presentation demonstrated that at least in the academic sector solutions for effective, secure identity management are possible over heterogeneous, mobile networks where multiple user roles co-exist (professors, researchers, students, etc.). What was also

made evident was the increased need for addressing identity management challenges and how, once these were solved, what would be the impact on greater mobility for people and extended benefits. A number of questions were raised in the ensuing discussion such as: (a) can any of the lessons learned be used to reach consensus on standards and interoperability decisions?; (b) is the technical academic environment aiding in the identification and implementation of appropriate solutions?; (c) does the spirit of collaboration inherent among researchers help lower the 'trust' barriers to common solutions?. It was repeatedly stated that the existence of common goals (the so called Bologna process) acted as a catalyst in achieving consensus, which is not the case in industry or even government and that the research spirit helped through the creation of smaller more human-relation based communities.

Pawel Rotter (IPTS) still on the same theme of how new identification technologies could facilitate greater mobility, presented on "RFID as a tool for e-Identity management in a mobile world". This presentation briefly introduced RFID (active and passive tags from technical point of view), ICAO specifications for e-passports and the time schedule for e-passports implementation for EU countries and US. Electronic passport is the token facilitating the mobility of citizens; more precisely it allows travelling across the world and RFID is the technology that enables a more efficient mobility due to both its contactless and automatic aspects for identification control. However, Mr. Rotter underlined that the use of RFID raises some threats, such as personal data copying, profiling and relay attack and mentioned the possible identity-related consequences: identity cloning, identity fraud and also privacy violation. So, the main corresponding identity challenges are Data protection and Privacy. The presentation concluded by recommending that: (i) we should prevent data leakage at every point of the e-passport control chain (c.f. chain of trust concept) by applying protection techniques (e.g. anti-skimming material); and (ii) we should ensure that similar kind of protection is applied to any other type of electronic document with RFID issued in future.

The presentation identified the need for appropriate risk and impact assessment to help improve our understanding of the role of RFID technologies in influencing mobility of citizens. From the presentation, some open questions were raised relating to the nature of RFID technology and its use in e-passports: (a) who should be allowed to read e-passport? (national administration, banks, airlines, private companies, etc.); (b) how to ensure protection of data stored by these institutions?; (c) should another type of e-document be defined for use by private companies?; (d) should the standard range of 10 cm for RFID chip communication be decreased because of security?; and (e) is RFID more appropriate for e-documents than contact cards? In the discussion that followed, it was acknowledged that RFID-based tokens allow automatic identification but this also means that it is a passive process. Mr. Meints stressed the problem of unobserved and non-interactive (also called passive) authentication because this type of authentication does not allow the consensus of users to be obtained. Mr. Maghiros agreed but also underlined positive aspects of passive authentication: for instance convenience in the case of frequent flyers.

4.3.4 Session 4: Technologies enabling Mobility

Andreas Westfeld (Technische Universität Dresden) dealt with "Technologies Enabling Mobile Privacy." He presented privacy threats (e. g. from virus, malware) stemming from the

use of technologies enabling mobility and more especially from the vulnerabilities of the mobile devices (e. g. easy to be lost or stolen or lack of security). Mobile phones are becoming increasingly intelligent, and handsets are growing ever more like computers in functionality. Together with their communication capability, mobile devices will aim at the same level of insecurity against worms, Trojan horses, and viruses. Currently possible countermeasures like virus scanners are transplanted from workstations to mobile devices. However, current approaches for secure operating systems (microkernel or language based approach) can provide better protection of private information against malware. Mr. Westfeld presented the privacy diamond diagram (developed by University of Freiburg) and used it in order to describe the different configurations of linkability. He specifically demonstrated possibilities of un-linkability, requirements and solution proposals in order to achieve privacy protection.

In this presentation, mobility is defined by the use of mobile devices and/or internet, and the identified identity challenge is linked to data protection and privacy.

Carlos Rodríguez (IPTS) followed on and presented another mobile-enhanced technology, namely "Location-based Services (LBS): technological implications". Third and fourth generation cellular systems and alternative scenarios for short and long term mobile communications evolution were presented in an effort to identify emerging wireless technologies and at the possible convergence of mobile multimedia over integrated networks. He then went on to present LBS technologies and services. Obvious benefits and challenges (such as traffic versus location, property, storage, responsibility, cost, spam, data mining, consent, law enforcement) for society were presented. A number of open questions that should be addressed were also introduced, such as the protection of the user's identity, the differences between traffic and location data, the number of actors accessing location information and the possible introduction of a trusted third party.

4.4 Panel Discussions

Panel Discussion Relevance – The panel discussions were conceived so as to allow some synthesis of the various messages debated during the workshop. The target was to provide clear messages as to what is known and what still has to be studied for the benefit of all FIDIS partners. There were 3 panel sessions organised during this workshop, and in the following paragraphs the issues raised and the discussions that took place are presented.

4.4.1 "In what way is mobile authentication/identification different from fixed one? Are the users/organisations needs different?" How can you trust roaming users?"

Two major differences have been identified between mobile and fixed communication. The first one regards the area of identification and authentication requirements, while the second one is in the field of physical security. Other concepts that differentiate mobile user requirements relate to: (a) general restrictions on power consumption and for data input and visualisation due to the small size imposed on mobile devices; (b) the storing of confidential

data on the mobile devices which could more easily be compromised; (c) the restrictions of a single user operating system dedicated to mobile devices; (d) adapting solutions to heterogeneous network conditions, which means that there are also legal considerations beyond technical ones so as to allow users to perform their tasks and receive their (subscribed) services seamlessly through heterogeneous connections in a trusted environment.

Two more issues emerged from this discussion: biometrics are unlikely to impact significantly mobile authentication solutions for the next 5, probably 10 years owing to the energy requirements and the reliability limitations that these currently demonstrate; and there needs to be action on raising awareness of the mobile user on the capabilities/limitations of mobile services at least until such time as legislation and appropriate enforcement would allow user protection.

Among the challenges that mobile systems have brought, an increased threat was identified of viruses now making their appearance in mobile systems (e.g. in mobile phones).

A need to increase the awareness of the users regarding the capability of their mobile devices was also identified, in order to mitigate the shortcomings / negative impacts of mobile communications.

Finally, it was suggested that a common solution for fixed and mobile communications could be reached, since it is difficult to provide solutions for each scenario (fixed and mobile). Also, if different solutions are adopted for the fixed and mobile environment, heterogeneity would be increased, which perhaps may create a greater problem.

4.4.2 "The Services - the Users"

ICPP (Contribution to the discussion)

Opening the second discussion, M. Meints and C. Krause provided a couple of slides on "Four Sector Model of Markets for Mobile Solution" in order to initiate a discussion about the borders between different types of communication (eGovernmental, Professional, public and private). They also stated that these borders are not always definite and can become a little blurry.

This picture (extracted from this ICPP presentation) perfectly illustrates a point highlighted by S. Elaluf-Calderwood (LSE): *Some changes of individual behaviour appear, which are regarded as an impact of the mobility on the information society; in particular publishing some private information -- data mobility -- (e.g. by doing blog) without being aware of possible consequences.*

In the ICPP presentation, "data mobility" concerns the e-Bay profile, and the applicant did not realise that a future employer can use private data available in the public domain for professional reasons.

So the awareness will become an issue for the mobile user in order to know how to protect his personal data and to understand the risk of his actions. If it is considered as a new responsibility, education may play a role to increase the awareness of the lifestyle related to mobility.

Also, manufacturer awareness has been identified as important as well, in order to consider these issues before the implementation / manufacturing of the products, so as to embed appropriate measures/safeguards in the manufactured products.

It was also noted that people had to give their consent all the time for things they are likely to give their consent anyway (e.g. Licence Agreement with Microsoft when a user installs Microsoft Windows on his/her PC), have made them giving their consent easier, without reflecting on it much, thus weakening if not completely eliminating the process of the user considering the request before giving consent. On the other hand, it is an established law that the user should first be asked and give consent, so that this part cannot be avoided in fixed as well as in mobile systems.

It was further argued that there is a consideration of mobile publishing, with regards to its being more instantaneous, thus posing a bigger threat as it does not leave much time to the user to reflect on his/her action.

At this point the benefits in protecting our privacy were identified to include the following:

- Protection against incorrect conclusions, that may be derived based on our published information
- The missing ability of attackers to manipulate and control our identity in the public.

Also, a number of questions were raised in the context of the discussion mainly as a result of the mobility needs of users and the authentication and identification challenges thereof. The open-ended questions were meant to help raise awareness as to possible solutions. These were: (a) can any of the lessons learnt trying to raise consensus on standards and interoperability decisions be repeated?; (b) is the technical academic environment aiding in the identification and implementation of appropriate solutions?; (c) does the spirit of collaboration inherent among researchers help lower the ‘trust’ barriers to common solutions?. It was repeatedly stated that the existence of common goals (the so called Bologna process) acted as a catalyst in achieving consensus, which is not the case in industry or even government and that the research spirit helped through the creation of smaller more human-relation based communities.

4.4.3 "Mobility solutions: Threats, Risks, Mitigation" [J. Claessens, M. Meints, E. Kosta]

4.4.3.1 J. Claessens (Mobility solution by Microsoft)

Mr. Claessens presented the Microsoft solution structured around three axes: mobile services (integration planned in various stages), mobile platforms (management of a lot of devices at the same time) and technical platform mainly based on .NET solution. The main challenge is to perform mobile communications in a heterogeneous network of mobile devices in an instant way.

4.4.3.2 J. Claessens (Contribution to the discussion)

Mr. Claessens introduced an important topic on identifying ways to manage communications and data using mobile identity, while preserving privacy at the same time. He identified the two points in order to solve this complex situation: managing privacy (referring to identification information + location) and managing the complexity. He raised a question for discussion as to the possibility of configuring the user consensus only once, without having the user click "I agree" every time. He sees two disadvantages in users having to give their consensus each time:

- Much interruption and nuisance to the user
- A security problem, since the users are going to click "YES" in every question, without much considering the request.

From this introduction, some technical-legal aspects arose:

- Is it possible to adapt the "I accept" button concept (already existing in the fixed world) in the mobile world and still remain within legal boundaries? (related to consensus requirement)
- Negotiation tools/protocols (e.g. P3P was also cited) can help the non-interruption requirement but represent only one layer. However, it was estimated that few providers will be able to offer this type of tool: How could we avoid monopoly?

4.4.3.3 ICPP (Contribution to the discussion)

Mr. Meints first identified the following changes / considerations that have been generated with the introduction of mobile communications:

- They introduce a lot of personal data, locations, mobile devices etc.
- Simple contracts versus location-based, which could involve 4 or 5 generic participants in the communication, thus making it more complex.
- There is also the problem of transparency, the user of the data most of the times is not the controller of the data. In this case consent becomes very difficult to give, and the protection via pure legislation is difficult.

He believes Data Protection legislation is already strong with respect to mobile services (thus perhaps adequate for the time being), but its enforcement is rather difficult. In this context, he perceives a need to change the law enforcement and not the legislation per se. Also, since the

interpretation of the Data protection regulation seems to differ in the EU countries, he believes there is a need for consensus and standardisation in this matter. Consensus and standards in a European level could help to reach balanced competitive conditions on the European market. Additional legislation such as Works Council Constitution Act applies for the use of mobile services (in this case especially in the working context). So two questions arose:

- How can transparency of processes be implemented so that an informed consensus of the user can be achieved?
- How can security of personal data be technically achieved?

4.4.3.4 Eleni Kosta – ICRI-K.U.Leuven (Contribution to the discussion)

She brought mainly two issues into the discussion:

a. the proposal for a "Directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC" (hereinafter 'Data Retention Directive') and

b. answering the question 'How to prevent secondary effects: spam, fraud, inappropriate content for children, inconvenience in public space, etc?', Mrs. Kosta approached the issue of inappropriate content for children.

Specifically:

a. On 21.09.2005 the European Commission presented a proposal for a Data Retention Directive. This was the result of a long debate and disagreement with the Council, as to who is competent to issue such a Directive. A small introduction was made as to how long shall the data retention period last: e.g.

- Traffic and location data should be retained for a period of at least 12 months and not more than 36 (Council' draft framework decision on the retention of data […], dated 28.04.2004)
- Traffic and location data shall be retained for a period of 12 months up to 48 months (Council' draft framework decision on the retention of data […], dated 28.04.2004)[2]

b. During the discussion Mrs. Kosta presented four different approaches to the protection of minors against illegal and harmful content transmitted through mobile devices.[3] The harmful content may be legal content for adults, but harmful / inappropriate for children. The different approaches are:

---

[2] It is noted that the European Parliament has adopted on the 15th of December 2005 a directive on retention of data processed by telecommunications companies. The directive covers traffic and location data generated by telephony, SMS and internet, but not the content of the information communicated. The new EU law aims at assisting national authorities to track down possible criminals and terrorists by granting them access to a list of all telephone calls, SMS or Internet connections made by suspects during the previous few months. The directive will provide for data to be retained by the telecommunications companies for a minimum of six months and a maximum of 24. MEPs also added a provision for "*effective, proportionate and dissuasive*" penal sanctions for companies who fail to store the data or misuse the retained information.

[3] Based on the research of Eva Lievens, Legal Researcher at ICRI-K.U.Leuven

- Strict legislation (the paradigm of US Communications Decency Act & Child Online Protection Act)
- Special software or other Internet applications for Internet content monitoring (e.g. V-Chip or the Belgian 'SaferChat')
- Self regulation (e.g. UK mobile operators' code of conduct for the self regulation of new forms of content on mobiles)
- Co-regulation (e.g. Australian internet content regulation scheme). It involves both, mobile and internet operators, possibility to make on-line complaints and the intervention of government. Co-regulation requires cooperation between industries and government.

4.5 Lessons Learnt

As a result of the discussions and the presentations, a number of issues emerged that are important to note in the framework of FIDIS research. These are the following:

4.5.1 Mobile versus fixed identity: increased requirements and challenges

It is a conclusion stemming from nearly every presentation and agreed upon in the discussions: mobile and fixed identity has different requirements, the former presenting further challenges and considerations.

4.5.2 An increased need for mobility

It has also been an underlying notion within the discussions and presentations that there is an increased need for mobility for individuals and businesses, both in order to complete work requirements and to facilitate private, everyday communications and tasks. This increased need imposes further requirements mostly on the organisational part of mobile identity, such as consensus, awareness raising and procedural interoperability. It is not clear whether these targets can be achieved.

4.5.3 Identity challenges

The main identified identity challenges in a mobile world are:

- Data protection and privacy – Vulnerabilities multiply in a mobile world
- Identity portability – Maintaining you identity rights when using different platforms
- Identity roaming over heterogeneous networks – Heterogeneous aspect has to be preserved because it allows freedom for the users

Identity challenges at the European level are more difficult to meet also because of difference in the legislative framework between EU countries.

4.5.4 Key factor for mobile services success: Trust

From the different discussions, trust has been stressed as the most important factor in order to guarantee the success of mobile services. Trust is regarded as a bridge between mobile

individual and mobile usage or in other terms, a bridge between user requirements and mobile services. In the context of a mobile world, the concept of trust essentially is composed of transparency, consensus and user control.

4.5.5 Other challenges concerning mobility

- The need to redefine physical security; the solution must come from the user and not from the device?
- Mobile publishing, which is most instantaneous, and therefore does not provide the user with ample time for reflection of his/her actions
- Increased user and manufacturer's awareness regarding the capabilities of the mobile devices

The questions and issues raised in this workshop will be dealt with in WP11 and other Workpackages where mobile technologies such as RFID are analysed and discussed.

4.6 Dark Areas / Things We Do Not Know

- How to balance privacy and services' costs? How to protect and enhance privacy, while providing ease of use and minimum disruption to the user?
- How to securely and efficiently service "alien devices"[4]?
- How to achieve trust and standardisation, especially in highly heterogeneous and mobile environments? And if there are solutions towards this direction, are they only or basically technical?
- The implications of converging mobile and fixed technologies that may cater for mobile user requirements.

List of participants

FIDIS Members:	***IPTS people:***
• Martin Meints, ICPP • Christian Krause, ICPP • Denis Royer, JWG • Svetla Nikova, KULeuven • Eleni Kosta, KULeuven • Thierry Nabeth, INSEAD • Ammar Alkassar, Sirrix • Silvia Elaluf-Calderwood, LSE • Bernhard Anrig, VIP • Andreas Westfeld, Technische Universität Dresden • Joris Claessens, MS	• Ioannis Maghiros, IPTS • Pawel Rotter, IPTS • Carlos Rodríguez, IPTS • Barbara Daskala, IPTS • Sabine Delaitre, IPTS ***Other participant:*** ***Invited speakers:*** • Antonio Maña, University of Malaga, Spain • Diego Lopez, RedIRIS, Spain

[4] An "alien device" is a device which does not belong or is not recognised by the local network where it operates, and yet it is not hostile (e.g. it may belong to the network of the parent company provider).

5 Concluding Remarks

5.1 Methodology-related

The organisation of the integration workshops has enabled the multiplication of interactions, the raising of consensus and the development of a common knowledge base aiming at creating permanent links among FIDIS partner organisations. In line with the objectives of the FIDIS NoE, through these integration workshops, it was possible for FIDIS partners to come together, collaborate, exchange their knowledge and expertise, thus promoting and facilitating integration and networking.

Moreover, there was an opportunity to involve and combine subjects / issues from various Workpackages (e.g. WP2, WP5, WP11 etc.), on which participants exchanged information and expertise, and participated in relevant discussions and debates. It was thus possible to promote content integration between the various Workpackages of FIDIS, this being an important objective for the WP8.

Furthermore, in the context of these workshops, and especially through the discussions and debates, research gaps have been identified, that is, interesting points / areas for further consideration that had not been identified from the beginning, while deciding on the content of each workshop. These issues were and will be dealt with in the research oriented Workpackages. For example the FIDIS Deliverables D5.2a and D3.6 already deal with results and open issues from the first two WP8-workshops, for other Deliverables such as the first three Deliverables within WP11 and the biometrics related Deliverables in the third Workplan the integration of results of the second and third WP8-workshops is planned.

In relation to the organisation of the inter-disciplinary workshops a number of issues have emerged that created obstacles. The main one is that of attracting as many FIDIS partners as possible on a given day and for a given theme. Since there are so many events happening throughout the year (whether organised by FIDIS or not) it is always very difficult to attract speakers to these workshops. As a result the participation in the workshops involved not in all cases as many partner organisations as we intended.

Organising events well in advance will of course help in increasing participation. However, there is always a priority conflict between the speakers that have an important message to diffuse or a new topic to discuss and the attendees that can make it to the workshop on any given day. IPTS in trying to achieve its objective of enhancing integration among the Network of Excellence partners, was able to find an appropriate balance of speakers and participants for all three events organised.

5.2 Content

Apart from the methodology-related achievements, the integration workshops enabled the presentation and discussion of issues, such as identity theft, trust and mobility and identity,

towards the development of a common knowledge base and consensus, as well as towards the identification of knowledge and research gaps, i.e. issues that need to be addressed.

Specifically, through the presentations and discussion sessions that took place in the first workshop ("Preventing Identity Theft"), it was possible to give a definition of identity theft and also to provide technical solutions on the problem, thus assisting the integration of the diverse visions on identity theft and identity fraud. A number of technological solutions (such as RFID or Biometrics) were debated as to their potential to solve (or even soften) the problem.

In the context of the second workshop ("Identity emerging technologies and Trust"), a consensus was achieved with regard to the concept of trust: it is not only the result of a technological solution, but it involves several aspects, such as social, cultural and legal. Moreover, trust presents cognitive aspects; indeed, trust mainly is based on experience and reputation and is related to risk perception. Users need proof of trust. Also, some challenging issues to consider regarding trust where identified:

- Which data for authentication has to be stored and what is the role of standards?
- How to put in place efficient Trusted Third Parties and in which legal framework?
- How to define clear responsibilities?

Finally, in the third workshop ("Identity challenges in a mobile world"), a consensus was reached regarding: (a) the increased requirements of mobile versus fixed identity; (b) the increased need for mobility; (c) certain identity challenges in the mobile world, and (d) that trust is actually the most important success factor for mobile services. Moreover, some knowledge gaps were identified that could provide the basis for future work, such as:

- How to balance privacy and services' costs? How to protect and enhance privacy, while providing ease of use and minimum disruption to the user?
- How to securely and efficiently service "alien devices"?
- How to achieve trust and standardization, especially in highly heterogeneous and mobile environments? And if there are solutions towards this direction, are they only or basically technical?
- The implications of converging mobile and fixed technologies that may cater for mobile user requirements.