FIDIS

Future of Identity in the Information Society

Title:	"D11.1: Collection of Topics and Clusters of Mobility and Identity – Towards a Taxonomy of Mobility and Identity"
Author(s):	WP11
Editors(s):	Denis Royer (JWG, Germany)
Reviewer(s):	Mark Gasson (Reading University, UK) Mireille Hildebrandt (VUB, Belgium)
Identifier:	D11.1
Type:	[Deliverable]
Version:	1.00
Date:	Friday, 09 June 2006
Status:	[Final]
Class:	[Public]
File:	fidis-wp11-del11.1.mobility_and_identity.doc

Summary

This document gives an overview on the topic of mobility and identity and its related aspects (law, technology, sociology). Furthermore, it is the foundation for the work of FIDIS Work Package 11: "Mobility and Identity", defining its context and the initial terminology and concepts for the ongoing work of this Work Package. This document is primarily aimed at an audience of academics, EU policy-makers, experts in the fields of law, sociology, and technology, and other interested citizens.

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	30.09.2005	• Initial release (Denis Royer)
0.2	31.10.2005	• Halloween Release • Added first contributions to document.
0.3	11.11.2005	• Carnival Release • Redone parts of the Glossary • Added/Updated bibliography
0.4	20.11.2005	• General clean-up of document structure • Adapted citation style for contributions
0.5	21.12.2005	• Christmas Release • Added Key Terms chapters
0.6	06.03.2006	• Added contribution list • Cleaned up formatting and inserted updates of the authors • Added table of figures
0.7	10.04.2006	• Minor editing and formatting • Added updates of contributions • Updated bibliography
0.8	26.04.2006	• Added Executive Summary
0.9	21.05.2006	• Version for internal review
1.0	09.06.2006	• Finalised delivery version, including review remarks by: o Mark Gasson (Reading University, UK) o Mireille Hildebrandt (VUB, Belgium)

Contributing Partners:

1. Goethe University Frankfurt (Germany)
2. Vrije Universiteit Brussel (Belgium)
3. Unabhängiges Landeszentrum für Datenschutz (Germany)
4. University of Reading (UK)
5. Katholieke Universiteit Leuven / ICRI (Belgium)
6. Karlstads University (Sweden)
7. Technische Universität Berlin (Germany)
8. Technische Universität Dresden (Germany)
9. Albert-Ludwig-University Freiburg (Germany)
10. The *PRIME* Project – PRIME LBS Prototype

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. Executive Summary	Denis Royer (JWG)
2. Introduction	Kai Rannenberg, (JWG), Denis Royer (JWG), Andreas Westfeld (TUD), Sven Wohlgemuth (ALU-Fr)
3. Initial Scenarios	Marit Hansen (ICPP), Martin Meints (ICPP), Martin Rost (ICPP)
4. Mobility and Identity	Els Soenens (VUB)
5. Taxonomy and Data Protection Legislation	Eleni Kosta (K.U.-Leuven/ICRI), Nikolaos Volanis (K.U. Leuven/ICRI)
6. Technologies Relating mobile IdM	Christer Anderson (KU), Leonardo Martucci (KU), Sven Wohlgemuth (ALU-Fr), Mike Radmacher (JWG), Denis Royer (JWG), Tobias Scherner (JWG), Jan Zibuschka (JWG)
7. Conclusion and Outlook	Layla Nassary Zadeh (JWG), Denis Royer (JWG)
8. Glossary	All authors

Table of Contents

1 Executive Summary 10
1.1 Scope 10
1.2 Structure and Content 10
1.3 Purpose of this Deliverable 11
2 Introduction 12
2.1 Objectives of this Study 14
2.2 Structure and Content 15
2.3 Related Work: Deliverable D3.3 16
2.3.1 Protection of Identifying Data: Personal Data and Device Characteristics 16
2.3.2 User-friendly interface for the non-expert to prevent unintentional misuse 18
2.3.3 Verifiable linkage between real and digital identity on the user's device is important to prevent impersonation 18
2.3.4 Published identifying data must be protected against misuse by peers 18
2.4 Key Terms & Glossary 19
3 Initial Scenarios for mobile Identity Management 20
3.1 Introduction 20
3.2 Introduction of the Scenarios and Analysis 22
3.2.1 Scenario 1: Mobile Communication in Private Life 23
3.2.2 Scenario 2: Mobile Craftswoman 24
3.2.3 Scenario 3: Mobile Collaborator in ICT Projects 26
3.3 Summary and Conclusions 28
3.4 Key Terms & Glossary 28
4 Conceptual and sociological issues of Mobility and Identity 29
4.1 Introduction 29
4.2 The Concept of Identity 29
4.3 Mobile Identity 31
4.4 The concepts of 'mobility' , 'mobile' and 'locational information' 34
4.4.1 The concept 'mobility' in sociology 34
4.4.2 Defining the concept of 'mobile' in relation to mobile technologies 35
4.4.3 Locational information 36
4.5 Mobile Identity Management 37
4.5.1 Management of Identities through the use of mobile devices 37
4.5.2 Management of Mobile Identities 38
4.6 Summary and Conclusion 40
4.7 Key Terms & Glossary 40
5 Taxonomy and Data Protection Legislation 41
5.1 Introduction to the European Legal Framework on Data Protection 41
5.2 Data Protection Terms 42
5.2.1 An overview of data protection terminology 42
5.2.2 Data Protection terminology in mobile networks 45
5.3 Basic Principles in Data Processing 46

5.3.1 Fair and lawful processing 47
5.3.2 Finality principle 47
5.3.3 Data minimisation principle 47
5.3.4 Data quality principle 48
5.3.5 Conservation principle 48
5.3.6 Data processed in line with the rights of the data subject 49
5.3.7 Confidentiality and security 49
5.3.8 Data transfer to countries with adequate protection 49
5.4 Conclusion 50
5.5 Key Terms & Glossary 51

6 Technologies Relating to mobile IDM 52

6.1 Anonymity and De-Identification in Mobile Networks and Mobile Identity Management 52
6.1.1 Identification in Mobile *Ad hoc* Networks 52
6.1.2 Frameworks for Identification in Mobile *Ad Hoc* Networks 53
6.1.3 Enabling Practical Anonymity in Mobile *Ad-Hoc* Networks 55
6.2 Delegation of Rights by Identity Management 57
6.2.1 Privacy and Delegation of Rights 58
6.2.2 Attackers and Privacy Threats 58
6.2.3 Privacy Criteria for Delegation of Rights 59
6.3 Privacy by credential-based Identity Management 60
6.3.1 Identity Management Systems 60
6.3.2 Delegation of Rights and Identity Management Systems 61
6.4 State of the Art Application Scenario: The PRIME LBS Prototype 62
6.5 Conclusion and Outlook 63
6.6 Key Terms & Glossary 64

7 Conclusion and Outlook 65

7.1 Conclusion 65
7.2 Outlook on WP11 Deliverables 66
7.2.1 D11.2: Mobility and Location Based Services (LBS) 66
7.2.2 D11.3: Economic aspects of mobility and identity 66
7.2.3 D11.5: Study on private and public access to identifiable location data 66
7.2.4 D11.6: Survey on Mobile Identity Management (& LBS) 67

8 Glossary 68

9 Bibliography 79

Table of Figures

Figure 1: Interdisciplinary aspects of Mobility and Identity. 14
Figure 2: Four possibilities for anonymity with a minimum of relations that must be concealed (dashed arrows) by the anonymity mechanism (Zugenmaier, A., 2005) 17
Figure 3: Identity of Alice composed of various partial identities (Clauß, Köhntopp, 2001). 20
Figure 4: Identity of Alice in mobile communication in private life scenario (scenario 1) 23
Figure 5: Identity of Alice in the craftswoman scenario (scenario 2) 25
Figure 6: Identity of Alice in the collaboration scenario (scenario 3) 27
Figure 7: An anonymous routing protocol 55
Figure 8: An anonymous overlay network 56
Figure 9: Prototype Version 1 - Architecture Overview 63
Figure 10: Mobile services and the transfer of partial identities. 66

1 Executive Summary

1.1 Scope

This document is primarily aimed at an audience of academics, EU policy-makers, experts in the fields of law, sociology, and technology, and interested citizens. It gives an overview on the topic of 'mobility and identity' and its related aspects (law, technology, sociology).

Within the context of work already undertaken by the FIDIS NoE, it is built upon the work of FIDIS deliverables "D2.1: Inventory of Topics and Clusters"[1] and "D3.3: Study on Mobile Identity Management"[2], by extending and broadening their content towards a taxonomy of mobility and identity. Furthermore, this document is the foundation for the work of FIDIS Work Package 11: "Mobility and Identity", defining its context and the initial terminology and concepts for the ongoing work of this Work Package and the common terminology of the FIDIS project.

1.2 Structure and Content

This document is structured in 6 main chapters, representing the different perspectives (legal, socio-cultural, technological, etc.) of the topical cluster of "mobility and identity".

Starting with *chapter 2*, a general overview is given and the relation to other deliverables of the FIDIS NoE is laid out. Also the motivation for this document as the initial starting point for the work of Work Package 11 is presented, linking the different fields to the work done in FIDIS. This should help to build a common view on the topic of mobility and identity – *towards taxonomy of mobility and identity*.

Chapter 3 describes the concept of partial identities and their application to mobility and identity relevant aspects in a mobile working environment. The presented scenarios are used to describe the connection between partial identities and the concepts of mobility and identity. Furthermore, the change of borderlines between communicational contexts is described, when specific partial identities are moved (e.g. work life vs. private live) or communicational contexts are shifted, due to a change of control of the partial identity.

In *chapter 4*, the sociological foundations and notions towards mobility and identity are laid out and described in detail (e.g. idem and ipse identity). Within this section, the basic concepts of mobility, identity, mobility and identity, identity management, etc. are described from the viewpoint of sociology, linking to the technologies being used for the management of identities, such as Privacy Enhancing Mobile Identity Management Technologies (cp. chapter 6).

The European regulatory framework and law perspectives towards the protection of an individual's privacy are the central topic of *chapter 5*. Here, the basic laws and regulations relevant for mobility and identity as well as the relevant terms are introduced and discussed, laying the focus especially on the processing of data, as the implications from this directives are important for e.g. location based services (LBS), etc. Furthermore, the issues towards the

[1] Deliverable "D2.1: Inventory of Topics and Clusters" is available for download on the FIDIS website at: www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.1_Inventory_of_topics_and_clusters.pdf
[2] Deliverable "D3.3: Study on Mobile Identity Management" is available for download on the FIDIS website at: www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.3.study_on_mobile_identity_management.pdf

digital projection of a user and the protection of the private sphere of an individual and its right of informational self-determination are further discussed in this chapter.

Chapter 6 aims towards the technological facet of mobility and identity, extending the concepts described in FIDIS deliverable D3.3. Here, technologies for the de-identification in mobile *ad-hoc* networks and the delegation of rights in identity management are introduced as application scenarios for mobility and identity. Furthermore, the PRIME application prototype is introduced, as a state of the art application scenario for privacy-respecting mobile applications.

The last chapter (chapter 7) gives an overview of the upcoming work of Work Package 11 on "Mobility and Identity" and its future deliverables:

- D11.2: Location based services (LBS)
- D11.3: Economic aspects of mobility and identity

1.3 Purpose of this Deliverable

This deliverable focuses on the topic of 'mobility and identity' and its related facets as initial starting point for the future work of Work Package 11 ("Mobility and Identity").

While FIDIS deliverable D3.3: "Study on Mobile Identity Management", primarily focuses on the technical dimension of mobile identity management, D11.1 aims to broaden the general scope of the discussions in WP11 in order to link the technical aspects to their societal context. This is done by means of an analysis of the central concepts of both identity and mobility, referring to relevant sociological literature and by means of an analysis or the relevant legal framework. As such this deliverable should provide the tools to build a common view on the topic of mobility and identity. However, due to the many interdisciplinary aspects (e.g. sociology, legal, etc.), this study cannot by exhaustive, but the foundation towards a taxonomy of mobility and identity.

Moreover, this study also serves as a collection of terms and definitions in order to build a common terminology, adding up to the definitions build by the work of FIDIS Work Package 2: "Identity of Identity". The described concepts and definitions will be integrated into the Wiki on Identity related Terms (FIDIS Wiki), in order to enhance the FIDIS identity concept towards mobility and identity.

2 Introduction

Looking at today's world, the management of identities is becoming an increasingly important factor for the interaction of different parties, such as organisations or people. As outlined in deliverable "D3.1: Overview on IMS", Identity Management Systems have evolved into several types and classes, which may help to distinguish their usage and their focus.

While identity management systems for the Internet are debated intensively, identity management in mobile applications has grown silently over the last 15 years (Rannenberg, K., 2004). Still – and to many surprisingly – the Global System for Mobile Communication (GSM)[3] is one of the largest identity management systems with more then 1.65 billion subscriptions, with the Subscriber Identity Module (SIM) infrastructure being the basis for many application oriented initiatives to manage identities. This SIM infrastructure was introduced with mobile communication networks, mainly GSM, and for the end of 2005 the GSM association reported 1709.2 million subscribers with GSM being the fastest growing communications technology of all time. The number of countries with a GSM system is reported as more than 200 (GSM 2006), which exceeds the number of UN member states (191 in May 2006 (UN 2006)) and also that of countries where the 'McDonalds' fast food chain is represented (119 in May 2006, McDonalds 2006).

Even without special technology support quite a few people use a variety of GSM mobile communication accounts (and the corresponding SIMs and telephone numbers) to manage different identities for e.g. private and business purposes. Moreover, the almost global dominance of the GSM standard for mobile communications and the high penetration rates that GSM systems reached in many markets have inspired quite a few initiatives to piggy-back on the GSM system and especially the SIM as platforms for identity management and related applications.

- Identity management can be integrated into the SIM-Hardware.
- Identity management can use GSM subscriber information as issued with the SIM.
- Identity management can use GSM subscriber information stored in the GSM network.

The first two approaches aim at supporting the ID management that already exists in applications by using the GSM infrastructure. The third approach expands the GSM ID and user management itself and allows e.g. new revenue models in mobile communications. All three approaches are described in (Rannenberg, 2004) and may be extended in Universal Mobile Telecommunications System (UMTS) networks.

It is interesting to analyse the reasons for the quietness of the growth of GSM subscriptions and mobile IDs. The main reason is obviously that the telecommunications business of the

[3] GSM used to be the abbreviation for standardisation committee "Groupe Speciale Mobile" of the European Telecommunications Standards Institute (ETSI), but is nowadays being used as abbreviation for "Global System for Mobile Communication" describing networks and standards according to the specifications that go back to the "Groupe Speciale Mobile".

1990s was mainly national, and within the respective country it was spread among usually not more than 2 to 10 players. Both market characteristics do not encourage international media coverage or sensational story-writing as e.g. the approach of a multinational company (Microsoft) to establish a internet-wide identity management and call it "[MS] Passport]". Another reason is that the view of mobile telephones as computers and consequently as Internet terminals is spreading only very slowly, and SIMs were not seen as the main asset of mobile telephone but more as a helper technology..

However the mobile Internet and the "*classic*" (fixed line) one are integrating ever faster now, and the mobile networks are becoming enhanced Internet networks. At least three factors are enabling this.

1. In the aim of offering seamless services regardless whether customers are at home or on the road Telecoms and their mobile partners or subsidiaries are collaborating closer than ever.
2. Also different sets of attributes (partial identities) are needed in different situations – and they can be made available due to the relative strength of the SIM card as a security token.
3. In more and more cases the context of a person and their situation are important for mobile communications, e.g. for filtering incoming communication.

Most of the trends outlined here are not just a result of the development of mobile communication technology, but of the role that the services play in society and business life and of their economical, socio-cultural and governmental consequences.

2.1 Objectives of this Study

Being the starting point of Work Package 11, FIDIS deliverable D3.3: "Study on Mobile Identity Management" mainly focuses on the technical dimension of mobile identity management and the related technological aspects (cp. chapter 2.3). However, this is only a very limited view upon this topical cluster. In order to broaden the general scope of the discussions within Work Package 11, this deliverable focuses on the other relevant aspects of mobility and identity, such as legal aspects and sociology (this study) or economic aspects (deliverable D11.3), in order to present other perspectives.

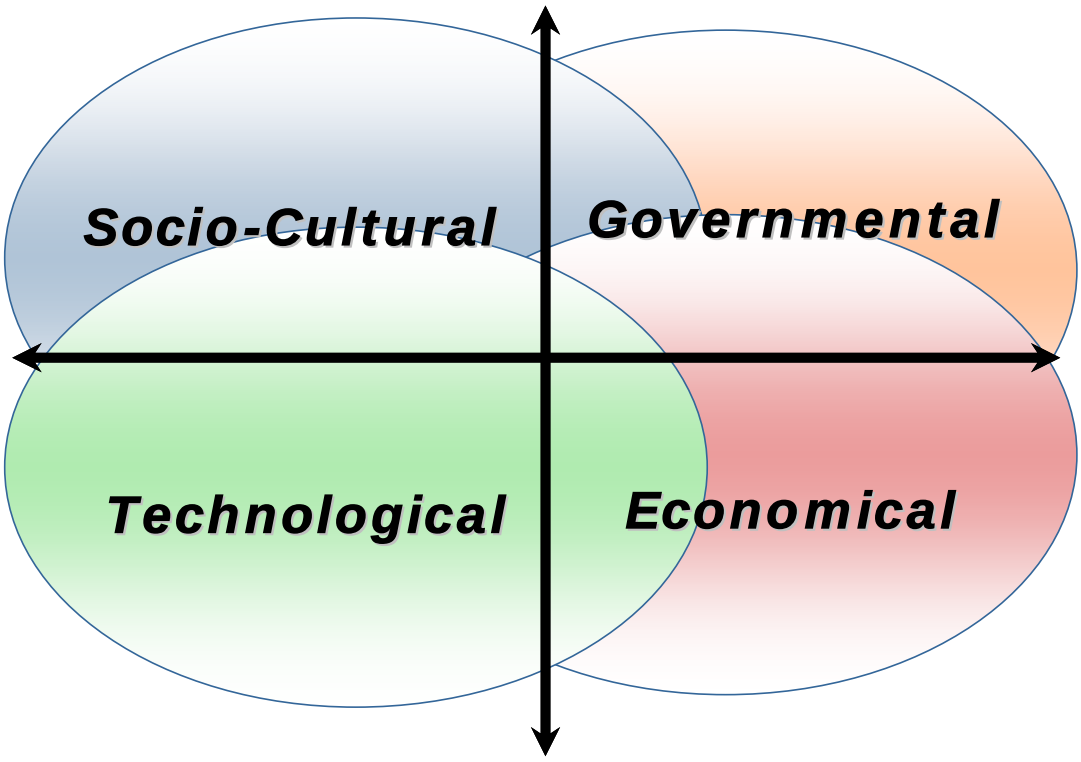


Figure 1: Interdisciplinary aspects of Mobility and Identity.

In general, the topical fields being identified and worked on in Work Package 11 include not only technological aspects, but also socio-cultural, governmental (legal, etc.), and economical aspects. However, each of these individual topics represents a microcosm for its own, allowing the identification of further overlaps and future research topics in Work Package 11 (cp. chapter 7.2).

Furthermore, looking at Figure 1, one can easily see that the presented clusters have a lot of overlap with each other. Therefore this study should serve as the foundation for the future work of Work Package 11 and as an initial collection of the relevant topics and clusters. Furthermore, this is done to identify and to show the interdisciplinary aspects, linking the different fields to the work done in FIDIS. Also it should help to build a common view on the topic of mobility and identity – *towards taxonomy of mobility and identity*.

Last but not least, it is the collection of the relevant terminology, adding its finding to the FIDIS identity concept and the terminology being edited by Work Package 2 and the Wiki on Identity related Terms (FIDIS Wiki).

2.2 Structure and Content

This document is structured in 6 main chapters, representing the different aspects of "mobility and identity". Starting with chapter 2, the general overview of the D11.1 document is given and the relation to other deliverables of the FIDIS NoE is laid out.

Chapter 3 describes the concept of partial identities and their application to mobility and identity relevant aspects. This serves as an initial scenario, being used to describe the connection between partial identities and the concepts of mobility and identity.

In chapter 4, the sociological foundations and notions are laid out and described in detail. Within this section, the concepts of mobility, identity, identity management, etc. are described from the viewpoint of sociology, linking to the technologies being used for the management of identities.

The regulations and law perspectives towards the data protection Legislation are part of chapter 5. Here, the basic laws and regulations being relevant for mobility and identity are introduced and discussed, laying the focus especially on the processing of data, as the implications from this directives are important for example for location based services (LBS), etc.

Chapter 6 focuses on the technical aspects of mobility and identity, introducing concepts for the de-identification in mobile *ad-hoc* networks and the delegation of rights in identity management. Finally, the PRIME application prototype is introduced, as a state of the art application scenario for privacy-respecting mobile applications.

The last chapter (chapter 7) gives an overview of the upcoming work of Work Package 11 on "Mobility and Identity" and its deliverables. Finally, all chapters of this study contain a section, stating a list of key terms and acronyms, being used in the individual chapters, in order to enhance the overall readability. The explanations and definitions of the terminology, being used in this study, can be found in the glossary (chapter 8). Furthermore, the terms are also available in the Wiki on Identity related Terms (FIDIS Wiki)[4].

[4] Currently the Wiki on Identity related Terms (FIDIS Wiki) is being build up by the FIDIS NoE. The current working version is available here: internal.fidis.net/fidis_wiki.0.html?&tx_drwiki_pi1[keyword]=WP11.

2.3 Related Work: Deliverable D3.3

An initial starting-point for this document and the other deliverables of Work Package 11: "Mobility and Identity" was the technical survey on mobile identity management of deliverable D3.3 "Study on Mobile Identity Management". It focuses on mobile users, which have a personal communication device, e.g. a smartphone or portable digital assistant with wireless connectivity, and on how identity management empowers them to protect their privacy. The key messages of this study are:

- Protection of both identifying data: Personal data and device characteristics.
- User-friendly interfaces need to be developed for the non-expert to prevent unintentional misuse.
- Verifiable linkage between real and digital identity on user's device is important to prevent impersonation. Published identifying data must be protected against misuse by peers.

2.3.1 Protection of Identifying Data: Personal Data and Device Characteristics

The transformation of the right of self-determination on information to the digital world requires (digital) anonymity mechanisms. Unless there are fundamental flaws in the implementation of anonymity mechanisms, the effect of profiling will be restricted, i.e. profiled information cannot be linked to a single person. Since it is hard to prove anything against profilers, the data protection legislation and the required unambiguous consent is difficult to enforce. In our opinion it is a misbelieve that personal data will not be profiled if no consent is given. Even if a company is not profiling, personal data may become public knowledge due to technical defects in the access control. A possible illegal profiling by third party can neither be prevented nor revoked. Hence, we should take action to minimise the acquisition of information that is possible by profiling not only by legal measures (cf. chapter 5). There are already mechanisms which enable the user to perform transactions anonymously. This is a prerequisite for users who do not like to give away their identity and other personal data that emerge as tradeable goods without anything in return. Due to the increased mobility we have to consider the question of how to guarantee the anonymity of the users of mobile devices.

As scenarios described in deliverable D3.3 have shown, two types of identifying data arise:

- Personal data that identify the end user and
- Device characteristics that identify the end user's device.

These identifying data arise all the time because of the frequent usage of mobile devices. An attacker, which might be an untrustworthy service provider or an eavesdropper, is able to trace and identify a mobile user via the location of this user and the characteristics of his mobile device, e.g. IP and MAC address, or via disclosed personal data of the user. According to the TCP/IP reference model, different kinds of anonymity mechanisms are needed to prevent tracing a mobile user. Deliverable D3.3 presented the identity management system

iManager for the application layer, and the anonymity mechanisms *FLASCHE* and *mCrowds* for the transport, network and physical layer.

Zugenmaier derives requirements for mobile use that anonymity mechanisms have to fulfil to guarantee the anonymity of the user (Zugenmaier, A., 2005). He shows that the existing anonymity mechanisms like DC-networks, mixes, onion routing, and crowds do not fulfil these criteria, i.e. they are not suitable for mobile use if anonymity is required. Mobility was simply not considered in the design of these mechanisms.

The 'attacker model' of Zugenmaier considers the specific aspects of mobility, namely the separation of

- the device used to perform an action,
- the action itself,
- the user,
- and the place where the user and the device are located.

An attacker has certain possibilities to reveal the identity of the user via the relationship of these four entities. We can derive classes of possible anonymising mechanisms from the 'relationship model'. One of these classes (cp. Figure 2, upper left) is especially suitable for mobile use because it permits the use of a personal device as well as location-dependent optimisation in the network.

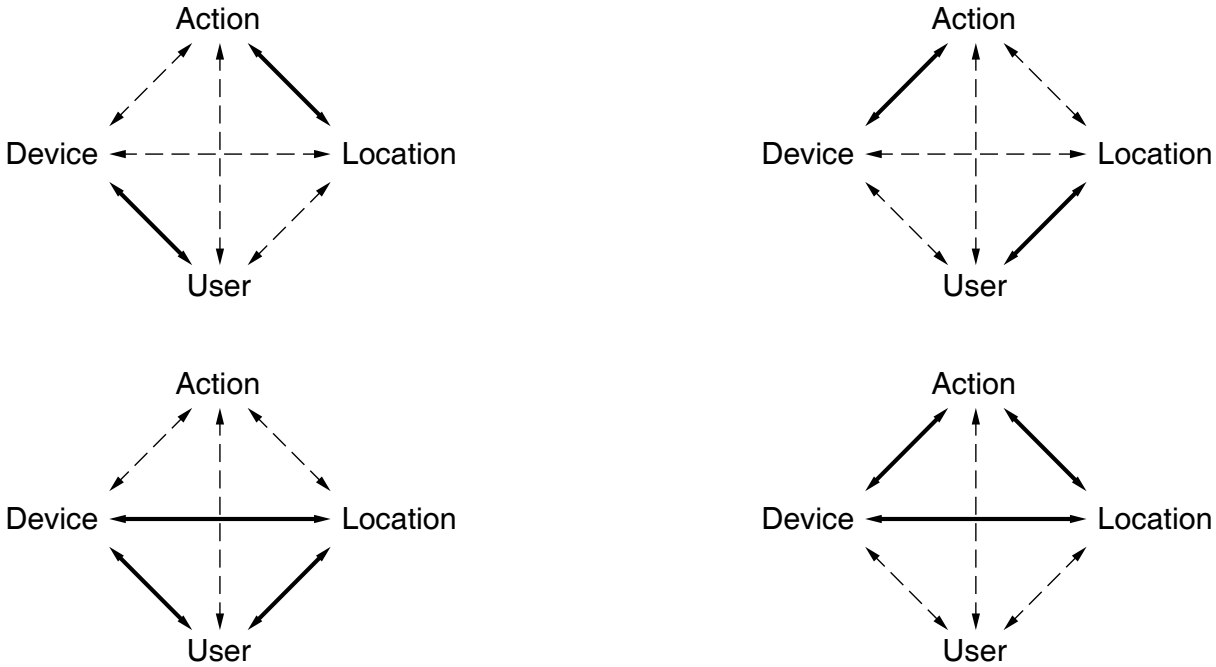


Figure 2: Four possibilities for anonymity with a minimum of relations that must be concealed (dashed arrows) by the anonymity mechanism (Zugenmaier, A., 2005)

The mechanism associated with this class is called 'location addressing'. It exploits the fact that the relationship between location and user as well as between location and device is not fixed because of the user's mobility. If the location of the user and the device cannot be linked to the user's identity, an attacker is allowed to know where an action is performed. However, the properties that identify the device or the user must be kept confidential. Since there are already mechanisms which ensure that a user does not reveal any personally identifying properties in an action, the location addressing mechanism only has to guarantee in addition that the device does not release any properties identifying the device itself.

One such mechanism (FLASCHE) was designed based on existing communication protocols. All identifying properties of the layers in the protocol stack have to be blinded, i.e. replaced by random values. The most important identifying property is the device address. Since an address is necessary to deliver a message to the right location, it cannot be completely random. The address of the device is derived from its location. This offers the possibility to optimise the routing in the network. The address also serves as a reference to assign a message to a connection and, hence, must not be changed during a connection.

2.3.2 User-friendly interface for the non-expert to prevent unintentional misuse

Security is not a primary goal of the user, i.e. users do not use security mechanisms in order to be productive. However, users underestimate the consequences of insufficient security and thus are rarely willing to invest a lot of effort in order to learn how to use these security mechanisms. Unintentional misuse of a security system by a user has a negative effect on the user's security. A mobile user has to configure anonymity and identity management systems if he wants to protect his identifying data. FIDIS deliverable D3.3 presents results from studies of P3P for mobile phones, (e.g. that the vocabulary of P3P is too technical to be readily intelligible for lay English users), and the managing of partial identities by using identity managers, such as *iManager*, for non-security experts.

2.3.3 Verifiable linkage between real and digital identity on the user's device is important to prevent impersonation

A user manages his identity or partial identities (FIDIS deliverable D2.1 - Nabeth, Hildebrandt, 2004) on his personal device. If his device is stolen, the thief has access to this identity and is therefore able to impersonate the user. It follows that the digital identity of a user has to be protected against unauthorised access. An approach for authentication of a mobile user is to link his real with his digital identity by using biometrics. With regard to this topic, FIDIS deliverable D3.3 presents a biometric authentication systems based on a smart card.

2.3.4 Published identifying data must be protected against misuse by peers

The anonymity and identity management systems presented by FIDIS deliverable D3.3 empower a user to control the disclosure of identifying data. This follows the principle of data economy. Business processes with personalised services and services acting as a proxy for a mobile user require a disclosure of identifying data and access rights of a mobile user to these services. Besides linkability, privacy threats of sharing disclosed attributes of a user without

his consent and misusing these attributes arise. This deliverable D11.1 investigates potential privacy threats while delegating access rights from a user to service providers.

2.4 Key Terms & Glossary

This is list of key terms and acronyms, being used in this chapter. For explanations, please refer to the glossary in chapter 8 or the Wiki on Identity related Terms (FIDIS Wiki).

- iManager
- Linkability
- Global System for Mobile Communication (GSM)
- MAC Address
- Subscriber Identity Module (SIM)
- TCP/IP
- Platform for Privacy Preferences Project (P3P)

3 Initial Scenarios for mobile Identity Management

Contributor(s): Marit Hansen (ICPP), Martin Meints (ICPP), Martin Rost (ICPP)

3.1 Introduction

This chapter uses the model of partial identities described in the FIDIS deliverable D2.1 (Nabeth, Hildebrandt, 2004). Following this model, the Me-related part of the identity of a person can be described as a number of various partial identities which are used in various communicational contexts.

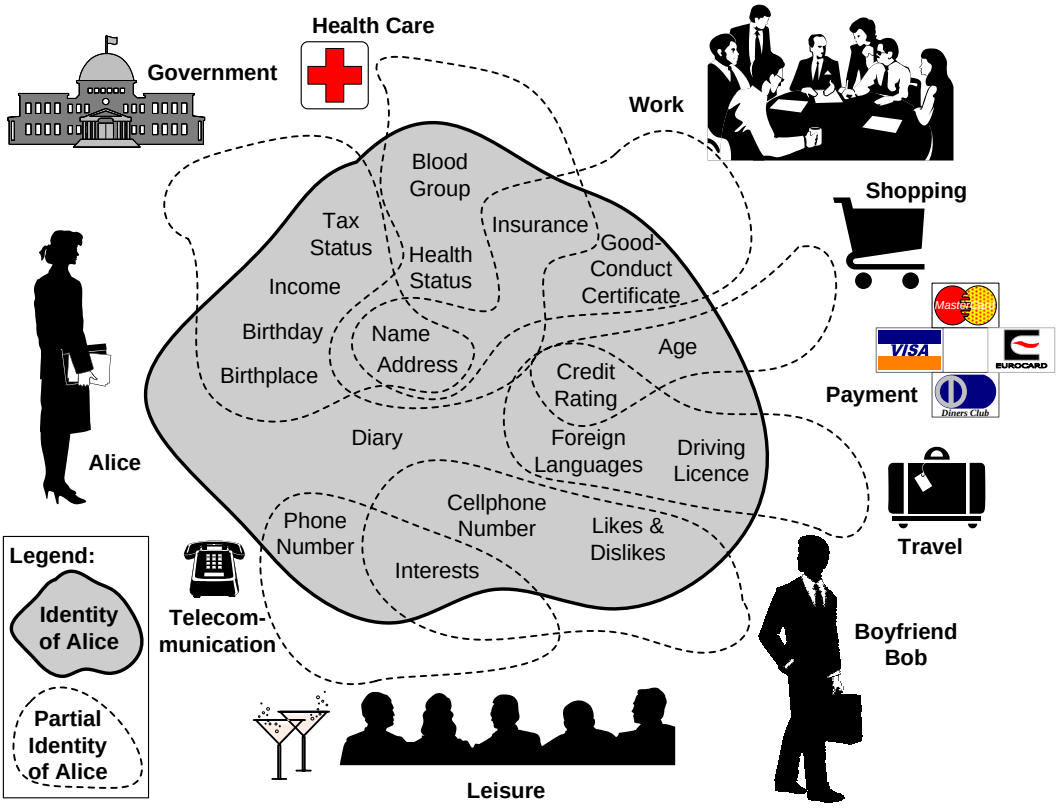


Figure 3: Identity of Alice composed of various partial identities (Clauß, Köhntopp, 2001).

Casassa Mont (Casassa Mont, 2004) describes identity using the formula "identity = data + policies". In further developing this model by introducing identifiers we distinguish between three important factors having influence on partial identities:

- Data including one or more identifiers (especially in the function of an address for communication) representing the partial identity
- The workflows or processes in which the data including the identifier(s) can be used
- The policy for the communicational context - how to use the identifier(s) and in which workflows or processes

Data in many cases is subject to modifications when used or processed in workflows and processes. While identifiers in their function as addresses are usually static at least for a certain time such as in the case of a phone or insurance numbers, workflows, processes and policies can differ widely. They are influenced on a macroscopic level by social systems and on a microscopic level by social structures such as the socio-cultural environment of the organisation they are used in. We observe in many cases interdependency between workflows and processes on the one hand and policies on the other hand. For example, when an organisation provides an infrastructure for its members for communication such as telephones for employees, it (in most cases) sets the policy dictating when and how this infrastructure can (or should) be used.

Data including an identifier can be used in many workflows, for example a mobile phone number that is used in both private and work related communicational contexts. The relationships between workflows and policies can be more complex. One workflow spanning two organisations for example can be subject to two policies. In turn a global communicational policy can be applied to different workflows within an organisation. The proper use of data and identifiers, the selection of an appropriate workflow and the compliance to the relevant communicational policy (or policies) is one of the challenges in identity management.

Using this model, we will describe the changes caused by the use of mobile communication and related partial identities in two general communicational contexts[5]:

- The private life and communicational contexts involved therein.
- The professional or work life and communicational contexts involved therein.

Within these general communicational contexts we can distinguish specific communicational contexts, which are directed towards specific communication partners. For example, within the general private communicational context we have a number of specific personal contacts (and thus contexts) including for example Alice's boyfriend Bob[6].

Traditionally, most people in Europe tend to stay for most of their lifetime in one village, town, or in a not too big region - their place of living. In these cases their private life is focused on personal contacts and specific locations such as a preferred pub, specific shops, the place of work, their home and so on, in that village, town or region.

In most cases fundamental and frequent changes in that place of living is caused by work. For many centuries mobile work was carried out, for example by craftsmen such as stonemasons, by mobile traders, mercenaries and others. Currently we observe that mobile communication plays an increasing role in mobile work. Mobile communication in that context is mainly used

[5] In order to reduce the complexity, typical additional contexts such as the communication with governmental institutions or the public life are not investigated in this chapter.
[6] The names Alice and Bob are commonly used placeholders for archetypal characters in fields such as cryptography and physics.

to increase the productivity of mobile work. In addition mobile devices supporting mobile communication, while offering much more functionality compared to a mobile phone such as smartphones, PDAs and notebooks are increasingly available (Weiss, 2005).

Current literature describes at least ten areas where organisational requirements have to be met by organisations introducing or using mobile work (Hess, Weddige, 2005). At least the five organisational requirements highlighted (bold) in the list below can have an impact on partial identities and thus the identity of a person in total. The requirements are:

- **(Flexible) Working hours**
- Accomplishments and control
- Health and ergonomics
- **(IT) Security**
- **Autonomy and flexibility**
- Qualification
- **Communication and contacts**
- **Private sphere and data protection legislation**
- Use of equipment by mobile workers
    - E.g.: Desk sharing, private equipment, etc.
- Liabilities and insurances

The implementation of these organisational requirements can show a big variety leading to very different impacts on the identity of persons. To analyse the impact on the identity of the person using mobile communication we are going to use three scenarios.

3.2 Introduction of the Scenarios and Analysis

For the analysis we selected the following scenarios:

- ***Scenario 1:*** Mobile communication in simple communicational contexts in private life (cp. section 3.2.1)
- ***Scenario 2:*** Mobile communication used by a mobile working craftswoman with fixed working hours (cp. section 3.2.2)
- ***Scenario 3:*** Mobile communication used by a mobile collaborator in information and communication technology (ICT) projects with flexible working hours (cp. section 3.2.3)
-

With respect to the management of identities these scenarios have a different focus. They refer to user controlled identity management (type 3 identity management, cp. Bauer, Meints,

Hansen, 2005) through the use of mobile devices, management of mobile identities and reachability management as an important method for user controlled identity management.

3.2.1 Scenario 1: Mobile Communication in Private Life

In the first scenario Alice buys her own mobile phone to use it for simple private communication only. The use of more complex communicational contexts such as the use of Location Based Services (LBS) will be analysed in Deliverable D11.2 "Location Based Services".

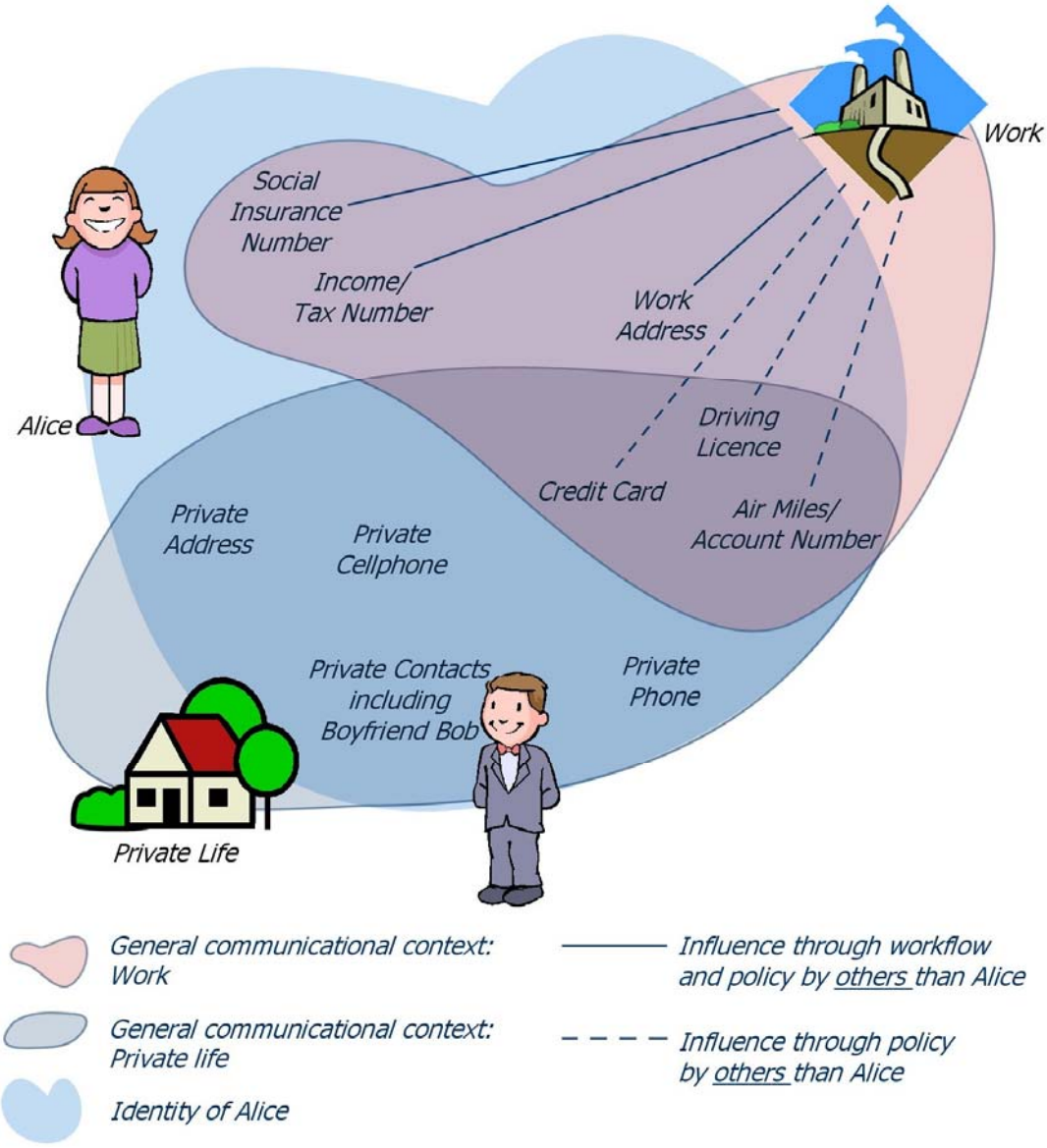


Figure 4: Identity of Alice in mobile communication in private life scenario (scenario 1)

With her own phone Alice is able to manage this new partial identity on her own. She can decide to whom she releases her cell-phone number (in this case her boyfriend Bob) and thus is able to use it for communication. In addition she is able to decide who is able to reach her using the mobile phone – when called, she can decide to answer it or not. So she has control

over the communicational policy and the workflows in which her mobile phone can be used. As the location of Alice in this scenario has no specific impact on the corresponding partial identities Alice performs type 3 identity management (user controlled identity management, cp. Bauer, Meints, Hansen 2005) using a mobile device (see also chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**).

In this scenario there is little change in the identity of Alice. Her cell-phone and related data (including the cell-phone's number) is now an additional partial identity (see ***Figure 4***) under her control and used in communicational contexts of her choice. The responsibility for the security of the data stored on the mobile device clearly remains with Alice.

3.2.2 Scenario 2: Mobile Craftswoman

In the second scenario Alice is working as a craftswoman with fixed working hours per day. Within one working day she is doing different small jobs at different places. She uses a mobile phone for professional purposes (in addition to her private one) in her working hours only to report to her employer and to get new jobs via phone when the old ones are finished. In addition, her employer uses the phone to contact her for internal control and planning purposes, i.e. how far she has got with her current job. (In addition, he carries out regular control visits at the various sites of her work.)

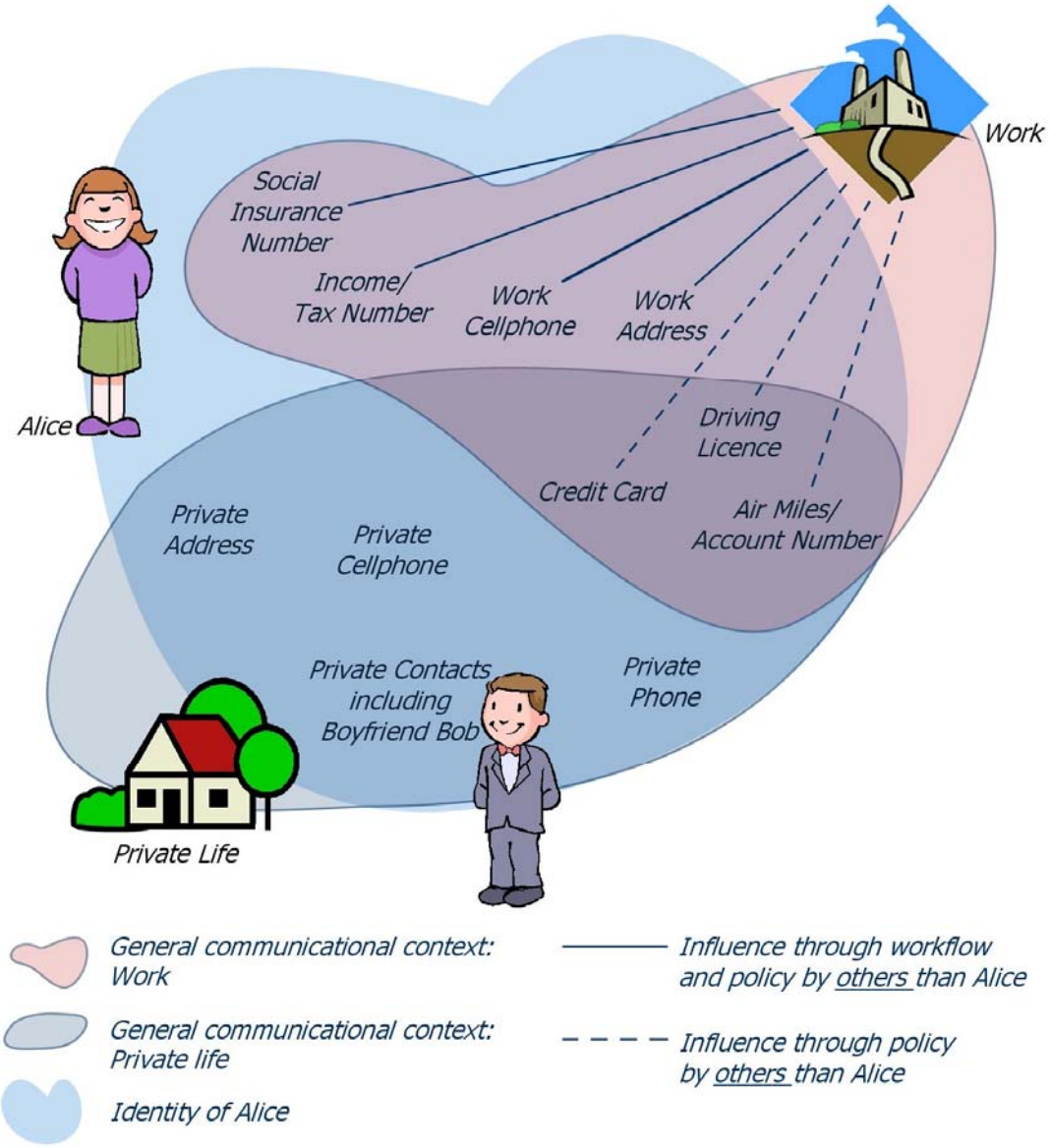


Figure 5: Identity of Alice in the craftswoman scenario (scenario 2)

An additional partial identity, the number of her cell-phone used for her work, is added to her identity in this scenario. In contrast to her own phone the communicational policy of her professional phone and the workflows in which it is to be used are controlled by her employer. In this case it is used in a restricted way for working purposes and in her working hours only. In addition within the management process of her work related partial identity the location plays an important role though the collection and transfer of the location data is not performed technically. In this context we can speak of management of mobile identities (see chapter 4.5.2).

Mobile communication is used as one instrument among others to apply a strict control to Alice's work. The resulting, almost non-existing, amount of autonomy certainly affects other partial identities used in the same communicational context in a negative way. For example, her reputation within the enterprise she is employed at and towards the customers of this enterprise may be affected ("Ah, Alice again – she has to be supervised closely.").

The resulting identity of Alice is shown in ***Figure 5*** which now comprises also a work cell-phone.

3.2.3 Scenario 3: Mobile Collaborator in ICT Projects

In the third scenario Alice is working as a collaborator in an ICT project. She works flexible and in some cases long hours and often stays at different places overnight. Her employer equipped her with a smartphone and allowed her to use it for private communication and contacts as well (which of course she has to pay for). Consequently Alice decided to give up using two mobile phones – she now only uses her professional smartphone.

The smartphone is also used to access certain services of her employer via web browser using an encrypted virtual private network tunnel (VPN tunnel) through the internet. Private and professional data stored on that device are encrypted; a root key to decrypt the data storage on the device is controlled by her employer. In addition private and professional data is stored on a central server as well under control of the employer (where they are not encrypted).

Within her area of work she has high flexibility and autonomy, but also responsibility for the results of the ICT project she is working on. Her employer follows a policy of open communication with his customers. As a result her mobile phone number is published on the internet and she is urged to answer the phone at any time in case customers call her. In turn her employer offers an extra payment (for example with a flat rate) for customer requests Alice answers when she is not working.

In this case the changes in identity are much more intense compared to the two prior scenarios. Highly flexible working hours in combination with the communicational policy of her employer lead to a change of borderlines of communicational contexts in which identifiers are used. In addition the control over those identifiers and the related communicational policies by Alice has diminished. When sitting in a restaurant with Bob having a romantic dinner she has to answer the phone when a customer of her employer is calling. This clearly has the potential to spoil the evening.

Offering the use of the official phone for private communication her employer increases the control on her private communication. He could possibly check her phone call numbers. Furthermore, her private entries in the phonebook are stored on the employer's central server where they are not encrypted with a key under control of Alice. Violation of data protection legislation by her employer may possibly have a negative impact for example on her reputation within the enterprise she is employed at, for example in cases where information about private dates leak out. This puts a light on possible challenges to implement data protection legislation when mobile communication is introduced in an employment context.

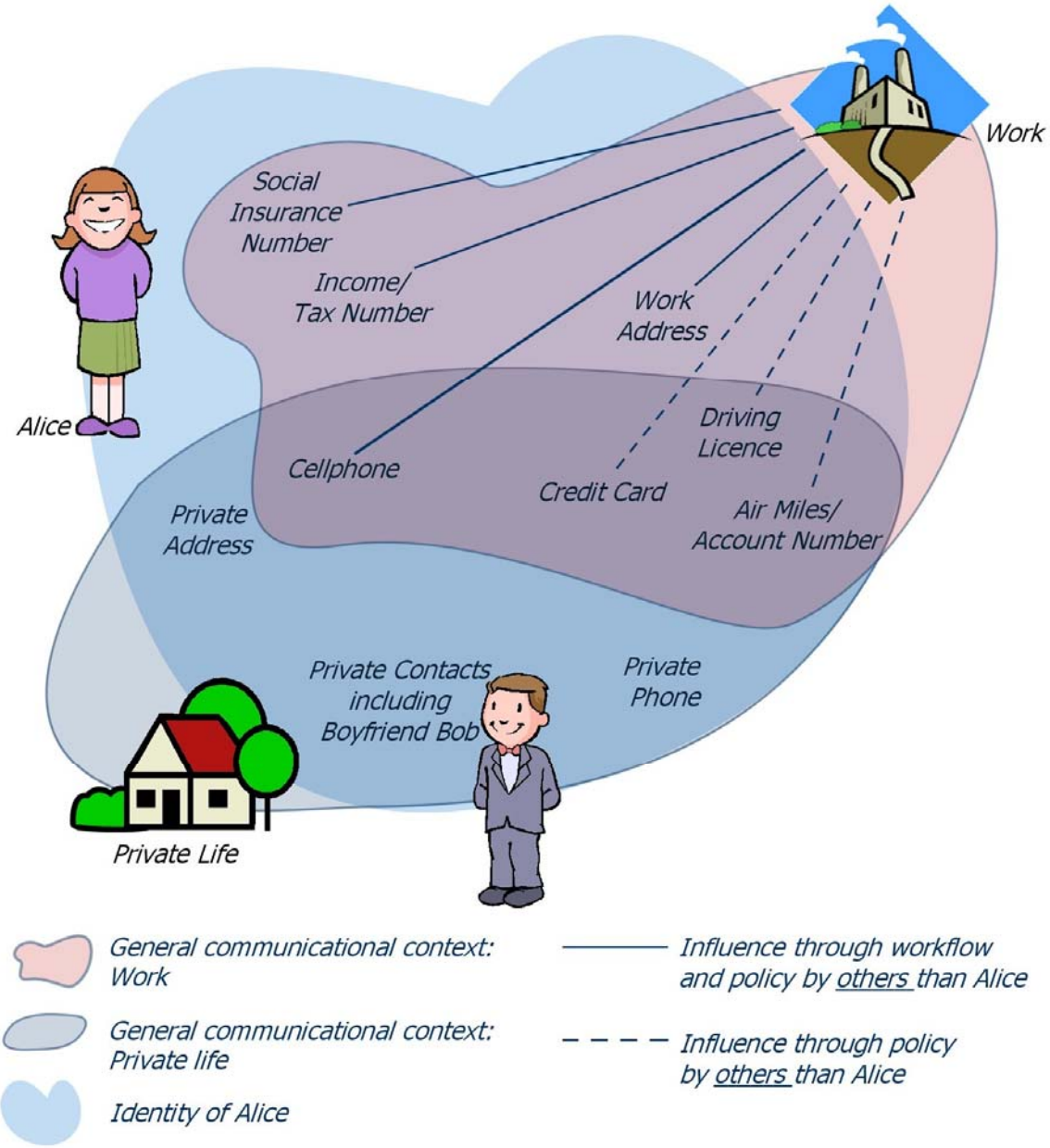


Figure 6: Identity of Alice in the collaboration scenario (scenario 3)

In addition, the combined professional and private data under control of her employer may be attractive for identity thieves. If the security of the central server (where data in this scenario is not encrypted) is insufficient and data from Alice is stolen, potentially severe trouble for Alice in both her professional as well as her private life may result, e.g. by abusing her data for stalking or fraud. In addition to the need to revoke and change (partial) identities, personal communicational contexts - for example with customers or friends - often suffer as well. Restoration of these communicational contexts, damaged by identity fraud, may need time and and may cause additional costs. In contrast to scenario 2 this may be more harmful because private communicational contexts are affected as well.

The resulting identity of Alice is shown in ***Figure 6*** now showing only one cell-phone to be used both for work and private life.

3.3 Summary and Conclusions

When working hours in mobile work are used in a more flexible way and in combination with mobile communication, partial identities previously used only in a specific communicational context can move into the mobile working context as well. This leads to a *change of borderlines between communicational contexts*. In contrast to private communicational contexts where the user controls the mobile communication-related identities, the workflows and policies in the work context are controlled mainly by organisations (in this case the employer). Mobile work in combination with both mobile communication and flexible working hours may shift, through the change in control and management of the identities, partial identities from user controlled, *own* ones to *assigned* ones.

In the scenario where Alice is a collaborator in ICT projects, there is a big difference between the communicational policy of the employer and the private communicational policy of the mobile worker. A centralised management of employees who are on standby for the enterprise in combination with Personal Reachability Management (Reichenbach *et al.* 1997) could probably be used as a central part of a Mobile Identity Management System (MIMS) in addition to an extra payment described in scenario 3 to balance these different policies and to protect the private sphere of the employees. In this context, MIMS are understood as being management systems for partial identities where the importance of mobility is prevalent (see Roussos, Peterson, Patel, 2003).

3.4 Key Terms & Glossary

This is a list of key terms and acronyms, being used in this chapter. For further explanations, please refer to the glossary in chapter 8 or the Wiki on Identity related Terms (FIDIS Wiki).

- Information and Communication Technology (ICT)
- Mobile Identity Management System (MIMS)
- Personal digital assistant (PDA)
- Policy
- Reachability Management
- Smartphone
- Virtual Private Network (VPN)
- VPN tunnel

4 Conceptual and sociological issues of Mobility and Identity

Contributor(s): Els Soenens (VUB)

4.1 Introduction

Mobility and Identity are the crucial topics in Work Package 11 of the FIDIS NoE. As deliverable D11.1 is the starting point of more elaborated explorations in the domain of mobile identities (in the next deliverables of the Work Package 11 of FIDIS), this chapter will provide some conceptual and sociological issues concerning identity, mobile identity, mobility and mobile identity management.

When developing technological and legal solutions in the domain of (mobile) identity management, it is important to keep in mind that mobile identity is usually perceived as an idem identity type. That type of identity shows only one side of identity. The ipse identity type and its relation with mobile idem identity should not be ignored. While in general technological and legal thinkers mainly concentrate on an idem mobile identity type, the aim of this chapter is to stress the link between idem identity and ipse identity building. When designing mobile identity management systems, it is important to keep this link in mind so that trusted, secured, privacy-protected and identity-friendly identity management systems in mobile applications and environments are designed, that empower citizens in the process of identity building.

This chapter is organised as follows: Firstly the concept identity will be discussed (cp. chapter 4.2); secondly the concept of mobile identity is discussed (cp. chapter 4.3). Mobility and mobile technologies are explored in chapter 4.4. Finally, section 4.5 discusses the concept of mobile identity management.

4.2 The Concept of Identity

The concept of identity is complex and different meanings are evident in different disciplines. In a multidisciplinary project such as FIDIS it is important to generate some common understanding between the disciplines involved. As such, enriched insights into the concept of *identity* are made here to assist in exploring the concept of *mobile identity* later on. The insights of Ricoeur (Ricoeur, 1990) and Beller and Leerssen (Beller, Leerssen, 2001) provide good starting points for an interdisciplinary investigation of the concept of identity.

Paul Ricoeur (Ricoeur, 1990) differentiates the *idem* identity type and the *ipse* identity type as ‘two sides of the same coin’. The idem identity type can be related to what other authors have called the “diachronic meaning of identity”, as it accentuates the permanence and continuity of an identity. As Beller and Leerssen remark: “*Identity becomes to mean being identifiable, and is closely linked to the idea of ‘permanence through time’: something remaining identical with itself from moment to moment*” (Beller, Leerssen, 2001, p.1). This type of identity is used in domains such as law, governmental affairs, profiling, marketers and assurances. Stressing

the idem identity type is attractive because of the possibility to identify an individual as "the same self" (Ricoeur, 1990). Stressing 'sameness' is important in these domains because one needs to categorise persons on the basis of certain characteristics. For example, "*In legal proceedings it is of paramount importance to establish a certain and continuous chain of identity for exhibits of proof and for the link between perpetrator and accused: 'this is the man who committed the crime last year'; 'these are the gloves found on the crime scene'*." (Beller, Leerssen, 2001, p.1). Sameness is based on comparison: no cognition without recognition. Human beings have the need to compare new information with what they already know. In fact, even unconsciously, people categorise information to identify risks and opportunities, for instance about people they meet, in order to decide how to interact with them.

By presenting people's identities as clusters of permanent and continuous categories, people can be identified, but does this mean that we 'capture' their unique identity? Though it seems evident that the idem type permits a useful conceptualisation in domains as law, marketing etc, from a multidisciplinary point of view this understanding of identity seems to be too narrow. Ricoeur and Belsen and Leerssen reveal 'the other side' of identity by referring to what Ricoeur (1990) calls ipse identity, which can be related to what Beller and Leerssen call the synchronic meaning of the concept of identity (Beller, Leerssen, 2001, p.1).

The synchronic meaning of identity refers to the 'unique sense of self' that a person has about his own being (Beller, Leerssen, 2001, p.4). Ipse identity concerns a first person perspective. This sense of self is continuously in development as one to fits one's auto-biographical narrative with the ever changing actions and reactions experienced in real life. The process of rewriting the story of your life enables you to reinterpret past experience and is essential for acting as a person with a sense of self in the present and the future. (Hildebrandt et al., FIDIS Del D7.4, 2005, chapter 3) We can refer to the work of the Norbert Elias, when he writes: "*individuals are humans in process. (…) Individuals are developing. And when we speak of a development, we mean the immanent order of continuous succeeding processes in which a latter shape results out of the former without interruption, (…) human is a process*" (Elias, 1970, p.130). So our ipse identity is social in that we need others to reconstruct our sense of self over and over again in life.

The ipse identity of a person cannot be captured in typologies of roles or in lists of fixed (group) characteristics used to describe the idem identity of individuals. In doing this, we would act as if the ipse identity is equivalent with idem identification. This is not the case, because the idem identity takes a more objective, or third person perspective. However, it is important to stress the link between the two types of identity. In constructing their 'whole outlook on life' (Elias, 1970) people are dependent on the idem identity types they perceive others to attribute to them. The way you are identified and categorised - by others and by yourself – does influence your ipse identity (Jenskins, 2003). In an advanced information society it could be the case that technologically mediated profiling practices, as they become ever more ubiquitous and are increasingly performed by unknown third parties, affect our

sense of self in a larger degree than profiling did before.[7] One of the values of our European constitutional democracy is the mix of positive and negative freedom that empowers citizens to take part in public life (positive freedom) and to retreat in their private realm (negative freedom, which includes some control of the access to personal information).[8] People need to enjoy this negative freedom in order to build a sense of self. This self-construction is mediated by the narratives we invent to tell the story of our life, which narratives are of course determined to a large extent by our interactions with others. However, from the point of view of the individual sense of self, as connected with human autonomy and dignity, citizens need a certain amount of control over the borders between self and others to flourish and partake in human society.

4.3 Mobile Identity

The definition of the concept of mobile identity used in FIDIS deliverable '3.3: Study on mobile identity management' provides us with a good starting point for further considerations in the domain. Citing the deliverable, a mobile identity can be defined as "*a partial identity which is connected to the mobility of the subject itself, including location data. The mobile identity may be addressable by the mobile ID. (…) Furthermore the mobility of a subject may be observed by others including the deployment of tracking mechanisms with respect to biometric properties, e.g., by a comprehensive video surveillance.*" (Müller *et al*., 2005).

It is important to keep in mind that in defining the central terms within a specific debate we may tacitly subscribe to a paradigm that implicates a whole set of decisions regarding the scope and nature of the domain we are investigating. For this reason the choice of paradigm is a decisive factor in research and especially in a multidisciplinary context such as FIDIS, it is important to reflect on the implications of our definitions. As Thomas Kuhn states paradigms are '*frameworks with shared beliefs values, assumptions and techniques which shape observation of reality.*' (Kuhn, 1962). Indeed, the chosen paradigm guides the selective perceptions. It may be the case that this definition is informed by a technocratic paradigm that underlies the common use of terms like digital identity, virtual identity and mobile identity (Saärenpaä, 2002) (Roussos, Peterson, Patel, 2003). In formulating mobile identity as a partial identity, we may employ a functionalistic point of view, which assumes that our personal identity is just the aggregation of our social roles in various social contexts. However, we think that our (ipse) identity is more than classifications of roles and the corresponding attributes (Castells, 1997).Therefore, we must be careful that we do not ignore the link with the ipse identity type when speaking about mobile identity. According to Saarenpaä the classical definition of digital identity is '*a negative definition*' towards the concept identity because 'the idea that identity is a composite of identifying information is misleading' (Saärenpaä, 2002, p. 20). Indeed, identifying people on the basis of data derived from their mobile devices only points to their idem identity and tends to ignore the effects onto the ipse identity. Without this differentiation, Saärenpaä has a point in referring to 'a negative definition'.

[7] See Hildebrandt M., Backhouse J., FIDIS Deliverable D7.2. 'Descriptive analysis and inventory of profiling practices', 2005, p 14 and chapter 4..
[8] See Hildebrandt M. et al. FIDIS Deliverable D7.4. 'Implications of profiling practices on democracy and rule of law', Chapter 3 'Profiling and the identity of European citizens' of M. Hildebrandt p 32 -34.

There is support for the idea that the concept of mobile identity as originated from deliverable D3.3 - should be seen as a *mobile idem identity and not as a ipse identity type,* while at the same time it is important to acknowledge the relations between the two types of identity.

Saarenpaä 's 'digital identity'

To argue that the presented concept of mobile identity concerns mobile idem identity, we can refer to the definition of digital identity of Saarenpaä. To him digital identity is '*a message which is received about a person through digital information either as such or in combination with other information of that person (characteristics, habits)*' (Saärenpaä, 2002, p.20). He states that by receiving digital information about a person, you receive a message about this person, but you do not capture an identity in the sense of an ipse identity.

Cameron's 'digital identity' and 'digital subject'

Other interesting comments on the conceptualisation of a mobile idem identity can be found in the writings of Kim Cameron (Cameron, 2005). Cameron distinguishes a 'digital identity' from a 'digital subject'. According to him, a digital identity is '*a set of claims made by one digital subject about itself or another digital subject*' (Cameron, 2005, p. 4). He further defines a digital subject as '*a person or thing represented or existing in the digital realm which is being described or dealt with*' (Cameron, 2005, p.5). The definition permits to take the idea of 'claims' into consideration when dealing with mobile identity, because of the fact that the digital identity is expressed through a list of 'attributes' related to the digital subject. As attributes are things expressed in claims, '*assertions need always be subject to doubt - not only doubt that they have been transmitted from the sender to the recipient intact, but also doubt that they are true, and doubt that they are even of relevance to the recipient.*' (Cameron, 2005, p.5). So, Cameron points out that 'digital identity' is about making claims. It stresses that attributes which are ascribed to a digital subject can be contested.

Roussos et allii: 'identification' and 'digitial self'

A third resource that can contribute to an adjusted conceptualisation of mobile identity is found in the paper 'Mobile Identity Management; an enacted view' by Roussos *et al.* (Roussos, Peterson, Patel, 2003). The authors make a distinction between identification and the digital self. Whereas they claim identification to be 'a static concept', the concept of the digital self "*is altogether more dynamic because it is arguably situated, negotiated and underpinned by trust*" (Roussos, Peterson, Patel, 2003, p.3). To Roussos *et al*, "*Identification is a restricted concept that refers to some combination of facets by which an entity is recognised. Digital identification is a set of data that represent the personal information of an individual or an organisation.*" (Roussos, Peterson, Patel, 2003, p 5). The concept of the digital self of Roussos *et al*. can be seen as the outcome of the interplay of someone's ipse identity and his various 'digital', 'mobile', or 'virtual' idem identities.

Based on these analyses, mobile idem identity can be understood as the result of categorisation of data derived from the use of mobile devices. Combining Saarenpaä and

Cameron, we can say that the 'messages' result in 'claims' which means that a mobile identity can be seen as a contestable representation of the (digital) subject (in the sense of Cameron). As the idem identity is about a core representation and thus – in the sense of Roussos et al. - about identification rather than about the sense of the self, we could refine the definition of Work Package 3 as follows: A mobile identity in the sense of idem identity is a message or a set of (linked) messages derived from mobile computing devices, constituting claims about the mobility, the location or other characteristics which are used to represent a data subject. Time, location, personal characteristics, location based authentication and pseudonyms thus contribute to constitute one's mobile (idem) identity.

As to the diachronic meaning of identity, we can say that it '*is of paramount importance to establish a certain and continuous chain'* (Beller, Leerssen, 2001, p.1) between the data subject and its location. Indeed, the discourse of many mobile identity services, such as the Location Based Services industry, is "*to capture once and for all the immediacy of the given self, to read off identity from location.*" (Harper, 2002, p. 9) Location Based Service providers may pretend that the representation of a data subject through the use of mobile devices reflects the subject's self, however mobile identity should rather be acknowledged as a (contestable) idem identity type.

While this analysis suggests that mobile identity must be seen as an idem identity type, it is also important to acknowledge that mobile computing devices can help people in their identity building and are thus part of the process of the ipse identity building. This is the case because these devices - with their capacity of managing communication and information – provide options for specific social interactions on an almost continuous scale (wherever, whenever, with whoever one chooses). In this sense, both the way you are presented through (the use of) mobile devices as well as the way others 'see you' and react to your messages, will influence your 'outlook on life' which may cause you to reshuffle the narrative of your life (introducing new contacts, whether private or professional; creating new preferences; being available to a much further extent when outside the reach of one's non-mobile phone). On top of that, profiling techniques which use information from mobile devices can have implications on the ipse identity, especially when this is done on a continuous, real time, invisible manner.

According to FIDIS deliverable D3.3, both GSM and Closed Circuit Television (CCTV) can capture the mobile identity of a person. For people communicating through their GSMs, their location need not be that important for the purpose of having a conversation (of course, location is at stake when one is in a location with no 'reach')[9]. Having a GSM enhances communication from almost everywhere at almost any time, which enables the user to have social interactions. Through these social interactions, one is able to change one's outlook on life. A CCTV is rather about the surveillance of a specific location, and only when you anticipate or know about the CCTV in an certain area, you can adjust your behaviour or appearance . This can have impact on your ipse identity as well. So both mobile identities,

[9] Of course to the service provider location is known, and the data retention regime stipulates that the data are saved for months.

that of a person using a GSM and that of a person being watched by CCTV could affect one's ipse identity. However, CCTV management schemes seem to bear a greater risk to the reciprocity and the understanding principle. This is an important fact, as these principles are essential for the freedom to build one's identity building in the ipse view.[10]

After exploring the concepts 'identity' and 'mobile identity', we can now have a closer look into the concepts of 'mobility' and 'mobile'.

4.4 The concepts of 'mobility' , 'mobile' and 'locational information'

4.4.1 The concept 'mobility' in sociology

In this section, first social mobility is shortly discussed. Secondly we look into 'mobility and social interaction'.

Social mobility

In social science, social mobility can refer to both horizontal and vertical changes or moves.

- ***Social mobility*** concentrates on changes in the socio economical status (SES). Social mobility can be the result of "*(1) structural changes in the working population, new positions become available or some positions experience a lack of people (there can be a demographical cause) or (2) efforts of individuals, to generate a certain position (e.g. educational level – importance of status gaining processes).*" (Vincke, 1998, p.265).
- ***Horizontal social mobility*** concerns, according to Sorokin (Sorokin 1959), 'transition of an individual or social object from one social group to another situated on the same level', while ***vertical social mobility***, '*refers to transitions of people from one social stratum to one higher or lower in the social scale*' (Sorokin, 1959)[11].

As to social mobility, it is interesting to note that there has been a shift in interest of marketers in the use of typologies. One very old fashioned but still used typology is the ABCD typology. The ABCD typology divides people into 4 categories on the basis of income. In the beginning, marketers were interested in the homogeneity of each class concerning, tastes, styles etc. Later on, they became interested in the movement of style patterns and preferences, beyond the class indicators. Social mobility was no longer something to control but something to investigate as 'source productive diversity' (Advirsson, 2004, pp.465-466). To use Urry's metaphor (Urry, 2000, p.186): there was a shift away from Bauman's gardener metaphor towards a gamekeeper vision.[12] This change in interest could reflect the diverse socio–cultural changes that occurred in the second half of the 20th century. As the overall wealth level of the populations increased and (catholic) morals became looser, people were freer to choose. In the spirit of capitalist societies, marketers learned that they would accumulate more if they could reach a broader mass for their products, instead of *a priori* ignoring the entrance of certain

[10] For an explanation of the reciprocity and the understanding principles see section 4.5.2
[11] Sorokin P., *Social and Cultural Mobility*. New York: The Free Press, 1959.
[12] Related to Bauman's Gardening metaphor, Urry (2000) accentuates the '*exceptional concern with pattern, regularity and ordering with what is growing and what should be weeded out*'. In the Gamekeeper metaphor it is about '*regulating motilities, with ensuring that there was sufficient stock for hunting in a particular site but not with the detailed cultivation of each animal in each particular place*'.

resources to fixed categories of people. According to Bennet and Regan, the idea of the 'mobile consumer' precisely points out that "*market research has come to regard all consumer actions and movement as having value.*" (Bennet & Regan, 2004, p.450).

Mobility and social interaction

In general, 'mobility is the ability and willingness to move or change'.[13] Nowadays, the (geographical) limits on social interaction, which have existed for so long, are declining very fast. In the light of the biological and socio–cultural evolution of human race, 'physical proximity' and 'stable dwelling places' were the basic conditions for people to engage in the very first complex human organisations. The horticulture of the Neolithic period or the irrigated valleys in Egypt and the industrialised urban cities all confirm this thesis. Over time, as the locomotion gave rise to the increase of spatial mobility, interpersonal communications were no longer sufficient to overcome distance. The landline phone decreased this gap by the end of the 19th century. However this technology implied the need to stay fixed with the landline phone to be able to communicate. But nowadays the mobile phone as Geser points out, "*makes communication compatible with spatial mobility.*" (Geser, 2004, p.5). Fortunati uses the term 'nomadic intimacy' (Geser, 2004).

For social science studies, movements and mobilities have become an interesting field of study, as Castells stipulates in his theory of the space of flows: "*our society is constructed around flows: flows of capital, of information, of technology, flows of organizational interaction, of images, sounds, symbols.*" (Castells, 1996). Being able to capture information about these flows becomes very important. The surveillance of flows and thus of mobilities (movements of people, cars, devices, data) is also important in the study of mobility and identity. Evidently the study of the movements of mobile identities as performed by surveillance technologies has profound implications for the ipse identities of citizens, employees, children, parents, etc.[14]

4.4.2 Defining the concept of 'mobile' in relation to mobile technologies

Related to mobility, 'mobile' refers to something that is able to move, so it is the opposite of 'static'. Bodies, transactions and artefacts have the ability to move. Besides, (wireless and wired) technologies have become ever more mobile. The well know expert in information technology and dataveillance Roger Clarke distinguishes four possible interpretations of the term 'mobile' in mobile technologies, which are presented hereafter (Clarke, 2003).

Firstly, 'mobile' can refer to movement to 'another location': "*Devices may be 'mobile' in the limited sense of being able to be in a different location at any given time from that in which they were at one or more previous times. Note that this can be the case not only with devices transmitting and receiving by wireless means, but also with devices that use physical connections, particularly* ***portables****, but also* ***handhelds****, and* ***wearables"*** (Clarke, 2003);

[13] www.wikipedia.com
[14] The link between idem and ipse identity is explained in section 4.2

Secondly 'mobile' can mean that transmission is possible from any location: "*pursuing the previous characteristic to its most extreme, the term 'mobile' could mean that a device could be anywhere, or, more carefully expressed, a device might be in any location from which transmission to another device is possible. Note that although there is a wide and increasing range of choices as to where to position a wireless device, there is also a great deal of scope for a relatively portable device that depends on an old-fashioned physical connection*" (Clarke, 2003);

Thirdly, 'mobile' can be relative to the earth's movement: "*a further interpretation of 'mobile' is in the more substantial sense of currently moving relative to the earth's surface, but nonetheless capable of sustaining data transmission, e.g., as a passenger in a plane, a train, a taxi, or a car, or, less safely, as the driver of a car. This is true to only a very limited extent with physically-connected devices. Note, however, that it is also only partially true in the case of wireless devices. That is because all wireless technologies have geographical limitations, and 'hand-off', e.g. from one cell to another, is fraught with difficulties*" (Clarke, 2003);

Finally, the term 'mobile' can point to devices that are portable and capable of wireless transmission: "*yet another sense of the term 'mobile' is to refer to devices that are designed to be easily and conveniently portable, and to rely on wireless transmission, possibly to the extent that they do not support cable-based connections.*" (Clarke, 2003).

As Clarke points out, mobile technologies are not *per se* wireless.

4.4.3 Locational information

Locational information is an important term in the context of mobile identities. What is meant by locational information? According to Bennet and Crowe (Bennet & Crowe, 2005), locational information is:

- ***'Geospatial:*** The position on the globe defined in terms of longitude, latitude and altitude.' (Bennet and Crowe, 2005, p 33)
- ***'Civic:*** The locational coordinates that are provided as a result of political decisions about border and boundaries made by international and state actors, such as time zones, country, street, postal address etc.' (Bennet and Crowe, 2005, p 33)
- ***'Descriptive:*** This category of locational information is referring to the type of location such as school, hotel, airport, city square, and so on'. (Bennet and Crowe, 2005, p 33) Note that, according to the authors, this category seems to be of interest to profilers since it adds important contextual information.[15]

[15] For more information about Profiling as a technology, a practice and a technique: see the deliverables of FIDIS Work Package 7: 'Profiling and its implications on privacy and security' (E.g. FIDIS Deliverables D7.2., D7.3., D7.4, 2005).

Location data does not imply that you are on the move. If one stays fixed for a period, this location may be registered as well Of course, each of your moves and movements can leave traces behind, with or without your knowledge.

After introducing some conceptual and sociological issues of identity and mobility, we can now explore the concept 'mobile identity management'.

4.5 Mobile Identity Management

Exploring the concept Mobile Identity Management at least two different *raisons d'être* can be discovered, depending on the choice of emphasis. These two different raison d'être are further elaborated in the following sections:

- Management of identity through the use of mobile devices (cp. 4.5.1)
- Management of mobile identity (cp. 4.5.2)

4.5.1 Management of Identities through the use of mobile devices

Firstly, mobile identity management can refer to the **management of identities through the use of mobile devices.** Here the fact that identity management is possible by means of mobile devices is stressed, not the management of mobile identities.

According to Josang *et al.* identity management is the "*process of representing and recognising entities as digital identities in computer networks.*" (Josang *et al*., 2005, p.1). Mobile technologies do not always disclose location data (Bennet, Crowe, 2005, p.9, also Clarke 2003). Therefore it makes sense to state that mobile technologies[16] which used for identity management do not necessarily regard mobile identities.

From the point of view of the end users, people can use mobile computing devices to facilitate their social interactions and their communications in a trusted and secured environment. We have to be aware that identity management systems (IMS) are at the same time "*the keeper of (...) personal electronic information*" and "*the channel through which individuals communicate, interact, transact, share reputations and create trust relationships with people, businesses, and devices.*" (Roussos, Peterson, Patel, 2003, pp.3-5). There is a possibility that the individual - independent of his or her mobility – uses mobile devices to manage social interactions in life, rather than managing mobility as such. In fact, Roussos *et al*. define identity management as "*the operations performed to support the lifecycle of the digital identity.*" (Roussos, Peterson, Patel, 2003, p.5). These operations are attempts to manage communication via the messages one sends or receives with mobile computing devices. So the management of identities through mobile devices stresses the importance of using mobile devices for one's identity management. This has implications to one's ipse identity - whether the person is mobile or not.

There are several reasons that support this position. First of all, we have to be aware of the fact that mobile technologies are used by individuals to regulate social interaction inside specific but interdependent figurations. In this sense, a person manages his identity in relation to his social interactions. Arguments can be found in the paper of Lasen: "*The use of mobile*

[16] For an understanding of mobile technologies see section 4.4.2)

phones depends on stable social infrastructures. (…) They are a tool for collaborative interaction in the local." (Lasen, 2002, pp.37-40). This stresses the importance of mobile devices towards the ipse identity aspirations, rather than towards enhancing mobility (Lasen, 2002, pp.37-40). Fortuniati (Fortunati, 2001) shares Lasen's opinion, who claims that: "t*he force of attraction of the device was beyond the constraints of mobile work or those of residential mobility*" and "*there was not a correlation between the mobility of the users and the use of the mobile phone.*" (Lasen, 2002, p.34).

From the point of view of the architects of identity management systems, especially related to the type 3 IMS[17], it must be ensured that the applications on mobile devices include Privacy Enhancing Technologies (PET) so that the end user can actually trust that he or she controls the data flows of the mobile devices used for identity management. As Hansen *et al.* (Hansen *et al*., 2004) suggest, privacy enhancing identity systems should be able to realise aspects such as:

- 'User controlled linkage of personal data'
- 'Data minimisation'
- 'Awareness of data being disclosed'
- 'Sufficient usability towards the user'.

4.5.2 Management of Mobile Identities

Secondly the concept of mobile identity management can refer to th**e management of mobile identities.** Here we stress the fact that the identities are *mobile identities*.

In FIDIS deliverable "D3.3: Study on mobile identity management" mobile identity management is described as "*a special case of identity management where location data is taken into account*" (Müller *et al*., 2005, p.78). This definition further distinguishes between the perspectives of the end user and the perspective at the organisational level. The definition stipulates: "*it comprises both the perspective of the subject whose partial identities are concerned, e.g., offering mechanisms to decide when and what location data is used and transmitted to whom and the perspective of the mobile identity (management) provider who operates the system and may process the subject's data.*" (Müller *et al*., 2005, p.78).

From the point of view of the end user, the management of mobile identity means that the end user uses computing devices to send or receive messages in which *location information* plays a major role In this case, the mobile computing device provides possibilities to use location based personalised profiles in interactions with others. Identity management related to Location Based Services also fall under this category. These uses create competing demands for identity management: from the point of view of the system provider, mobile identity management means that service providers must provide secured and trusted facilities to the

[17] 'Type 3 IMS are characterised by the user control as basically decentralised, user and client orientated': Bauer M. et al., FIDIS Deliverable D3.1 'Structured Overview on Prototypes and Concepts of Identity Management Systems", 2005, p14.

end user, while at the same time these service providers must enable the capture of the location data: "*it is used to … follow the user from device to device, location to location and context to context.*" (Roussos, Peterson, Patel, 2003, p.3).

To work out these competing demands we will use the 'enacted view' of Roussos *et al*. These authors approach "*mobile business as an open-ended socio-technical production: a mass of particular actions taken as individuals and groups make their own uses of technologies. The result may be dynamic, unpredictable and strongly mediated by the idiosyncrasies, needs, and preferences of individuals and groups.*" (Roussos, Peterson, Patel, 2003, p.3). The enacted view is to be embraced because it escapes technocratic determinism. It is a 'paradigm' which has *a fortiori* an eye for the social construction by which these mobile identity technologies are implemented and evaluated. The enacted view will provide better insights into the usability of devices and the trust in consumer–service-provider relations. Therefore we have to make sure that we build in various 'success factors' to succeed in creating user friendly identity management systems that can enhance trust between consumer and service provider. Indeed, system features which are crucial in relation to the ipse identity type are reflected in this enacted view of identity management systems, as it accentuates aspects such as the 'locality', 'reciprocity' and 'understanding' principle.

Towards the *locality* principle, the enacted view argues that there must be at least a "*balance between respect for the consumer's identities and the advantages of the 'open and ubiquitous mobile businesses.*" (Roussos, Peterson, Patel, 2003, pp.27-28). The locality principle thus entails that the user must be able to differentiate between the different partial identities one has taken up in various contexts. Furthermore, though personalised services can profit from the exchange of data between different commercial partners, this may lead to unwanted loss of trust by the consumers.

The second principle, *reciprocity*, deals with the "*informational (a)symmetry' between consumers and providers. This too is a necessary trade–off: 'a consumer may find profiling useful since it allows a personalised service to be offered but, on the other hand, it may be uncomfortable if the relationship is asymmetrical with regard to control and access to information. At the very least, the consumer should be remunerated for the informational asymmetry either directly or indirectly in a fair and acceptable to both parties way.*" (Roussos, Peterson, Patel, 2003, p. 29). In this sense the principle of reciprocity entails that people must know what data is collected about them, by who and what the benefits and risks of the data accumulation can be. Because the collected data can be used for profiling purposes, the authors feel that not only privacy concerns are important, but they refer also to the fact that the link to identity building must be acknowledged

Concerning the third principle, *understanding*, Roussos *et al*, claim that "*the perception of identity of the seller affects directly the perceived risk of the transaction, the willingness of the buyer to transact with the particular seller and last but not the least the price paid.*" (Roussos, Peterson, Patel, 2003, p.30). In this sense the principle of understanding entails that both consumers and providers should be able to understand each other 'identities'. This is the

case because, "*when this did not occur in the ubiquitous commerce scenario the consequence was that it created a threat for the balance of family structure.*" (Roussos, Peterson, Patel, 2003, p.30).

4.6 Summary and Conclusion

This chapter explored some essential concepts fundamental to Work Package 11 of the FIDIS NoE. Most importantly, we want to make explicit that the term mobile identity is mainly used as a mobile idem identity type. This means that in the process of identity building, people reflect about the mobile idem identities (which are third person perspectives) in order to constantly (re-) develop a sense of self (the ipse identity or the first person perspective). Related to mobile identity management, it is important to stress that when the end user is not able to control the digital or mobile identities ascribed to him or her, the positive freedom of self constitution and thus the ipse identity building may be 'limited' to a large extent. If one's negative freedom - including the opportunity to have some control of the access to personal information- is in danger because no 'enacted view' on (mobile) identity management is developed, then the self constitution of people is at stake, and this affects the European constitutional democracy. Therefore, referring to Roussos et al. (2003), aspects as locality, reciprocity and understanding must be integrated into Privacy Enhancing Mobile Identity Management Technologies.

4.7 Key Terms & Glossary

This is a list of key terms and acronyms, being used in this chapter. For further explanations, please refer to the glossary in chapter 8 or the Wiki on Identity related Terms (FIDIS Wiki).

- Biometrics
- Closed Circuit Television (CCTV)
- Cell
- Cell-phone
- GSM
- idiosyncrasies
- Idem
- Ipse
- Location information
- Privacy Enhancing Technologies (PET)
- Wearables / Wearable PC

5 Taxonomy and Data Protection Legislation

Contributor(s): Eleni Kosta (K.U.Leuven/ICRI), Nikolaos Volanis (K.U.Leuven/ICRI)

5.1 Introduction to the European Legal Framework on Data Protection

As Solove *et al.* have mentioned (2006, p.1) "we live in a world shaped by technology and fuelled by information". Indeed, as networks become more sophisticated and ubiquitous, the citizens are increasingly using their offered services in several aspects of everyday life such as business, education, information, entertainment etc. However, this growing use of telecommunication networks and technologies has brought the importance of the protection of data, resources and identities to the fore. The deployment of technologies that may cause significant harm to the citizens' right of privacy – RFID tags, biometrics, GPS and Location Based Services to name a few-, has raised far-reaching questions about the future of the private sphere and the informational self-determination of the users.

Central to this debate is the role of law. Legislative initiatives have already been taken so as to guarantee the right of citizens' privacy in an era of pervasive technological architectures. In this chapter, we present an overview of the European regulatory framework regarding the protection of privacy. The reader will also be introduced to the relevant legal terminology as well as the basic principles regarding the use of personal identifiable information. A general approach has been favoured instead of a narrowed and case-specific one, so as to facilitate the reader to understand the key concepts of the relevant legislative framework. Although specific references to the use of mobile technology are explicitly made in specific cases such as the use of traffic data or location based services, this chapter shall be rendered as an introduction to the general taxonomy of data protection legislation in the European Union

As a starting point, the fundamental right to privacy is recognised in article 8 of the European Convention of Human Rights and Fundamental Freedoms[18] which stipulates that everyone has the right to respect for his/her private and family life, home and correspondence. With the advent of new technologies however, the notion of correspondence, has acquired a wider perspective, and it has come to contain, in addition to its traditional meaning, any type of point-to-point communication realised through an electronic communications network. It follows that the notion of mobile communications networks is also covered by the scope of the article, being a *genus specialis* of electronic communications networks.

Important for the completion of the data protection regulatory framework are the initiatives taken by the Council of Europe. On 28.01.1981 the Council of Europe adopted the Convention for the protection of individuals with regard to automatic processing of personal

[18] Available online at http://www.echr.info/

data (Convention nr. 108) and on 08.11.2001 it adopted the Additional Protocol to the aforementioned Convention, regarding supervisory authorities and transborder data flows.[19]

In the field of European Union law, the Charter of Fundamental Rights of the European Union (hereinafter EU Charter)[20] provides for the respect for private and family life (Art.7) and the protection of personal data (Art.8), while two directives have been adopted to guarantee efficient data protection.

The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter called 'Data Protection Directive')[21] pursues two closely linked objectives: to lay down specific rights of the individual on his/her personal data but also to ensure that such data can move freely within the single market created between the Member States of the EU.

A second, sector specific Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter called 'ePrivacy Directive')[22] translates the data protection principles of the general Data Protection Directive into specific rules for the electronic communications sector, regardless of the medium used. This directive regulates issues, such as confidentiality of communications, status of traffic data, use of location based services, and unsolicited communications and therefore it should be taken into consideration, along with the relevant working documents and opinions of the Data Protection Working Party of Article 29 of the Data Protection Directive.

5.2 Data Protection Terms

5.2.1 An overview of data protection terminology

In the general frame of taxonomy, a short presentation of the basic terms related to data protection is deemed necessary. Therefore, the term 'personal data'[23] is defined as 'any information relating to an identified or identifiable natural person ('data subject')'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

[19] The text of the Convention and its Additional Protocol is available online at: http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG
[20] http://www.europarl.eu.int/charter/default_en.htm
[21] O.J. L 281, 23 November 1995
[22] O.J. L 201, 37, 31 July 2002. The ePrivacy Directive replaced Directive 97/66/EC of the European Parliament and the Council of 15 December 1997 on the processing of personal data and the protection of privacy in the telecommunications sector, O.J. L 53, 14 January 1998
[23] Art. 2(a) Data protection directive

Although the Data Protection Directive tried to harmonise the processing of personal data and the free movement of such data, there are still enough differences between the Member States with regard to the term of 'personal data' and especially when it refers to an 'identified of identifiable natural person'. Despite the efforts of the European legislator to give a pan-European meaning to this term, there is still a categorisation into 'relative' and 'non-relative' concept of personal data. According to the relative concept, data are 'personal' for someone who can link them to an identified individual, but not for someone who cannot make such a link. This approach seems to be supported by Recital 15 which states that the processing of sound and image data is only subject to the Directive if that processing is automated or if the data processed are contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question.

The concept of 'identifiability' plays an important role for the legal status of all not fully (or not immediately) identifiable data, such as encoded or pseudonymous data, as well as sound and image data and IP addresses.[24] The possibility of matching data processed by a computer to a specific person will depend on a number of factors, such as who is doing the matching and what their technical capabilities are, what type of data is involved, whether other data are available to aid the matching etc. As far as the Internet or other type of network that adopts an IP address architecture is concerned, the attribution of data to a specific person can be made easier with the implementation of static (instead of dynamic) IP addresses. Indeed, a fixed IP address is more likely to be qualified as personal data[25] in the same way as license plate numbers or telephone numbers have qualified as personal data by the national data protection authorities.[26]

In interpreting the term 'personal data', the most expansive approach should be followed. Recital 26 of the Data Protection Directive for example reads that in deciding whether data could be used to identify a particular person 'account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person'. Moreover, the term 'personal data' should include all data about a person (including

[24] Belgium for instance has created its own rules with respect to these categories of data, especially regarding encoded research data. It has adopted detailed rules on the processing for research purposes of fully identifiable, encoded (pseudonymised) and fully-anonymised data. With respect to the processing of IP-addresses, the Belgian Data Protection Authority (Commissie voor de bescherming van de persoonlijke levenssfeer) has taken quite a radical view stating that "the processing of data regarding IP-addresses, irrespective of whether they are temporary or permanent, falls within the scope of the privacy law given that it is possible and easy to trace the identity of the relevant person via the Internet-provider". Nevertheless, the far-reaching interpretation of the Belgian Data Protection Authority notwithstanding, the Belgian Council of State [the supreme administrative court of Belgium (Raad van state)] at least on one occasion has taken the 'relative' approach to identifiability, referring to the (im)possibility of identifying a natural person 'with reasonable means', and held that data are anonymous 'if from a whole of available data (e.g. town, age, hospital, period of hospitalisation) there is reasonably no identification possible' (Prime Project, D14.1.a, See also Decision No. 45.218 of 10 December 1993, Vl.T.Gez. 1993-1994, 281)

[25] The IP address attributed to internet users are considered as 'personal data', see Art. 29 Working Party, WP 58, Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6 (30 May 2002), available online at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_en.pdf

[26] Moukas, Al., et al, Agent mediated Electronic Commerce II: Towards Next-Generation Agent-Based Electronic Commerce Systems, Springer, 2000, p. 50

economic, professional etc. data) and not only data about the person's personal life (Dammann and Simitis, 1997, p.109). This breadth of the conception of personal data means that data is usually presumed to be 'personal', unless it can be clearly shown that it would be impossible to tie the data to an identifiable person (that is, unless the data is truly anonymous) (Kuner, 2003, p.51).

An argument often raised by European Internet Service Providers in order to avoid the application of data protection legislation is that from the time a user sends his/her data via the Internet, these data are considered 'public' and not 'personal' and therefore do not fall under the scope of the European data protection legislation. However the Italian Data Protection Authority (DPA) held that participation in Internet newsgroups does not render the e-mail addresses of the participants public and therefore their collection and processing is only allowing according to the data protection legislation. (Kuner, C., 2003, pp.52-53)

Although the directives do not include a definition of the term 'sensitive data', Article 8 of the Data Protection Directive describes them as '*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*'. This clarification is of seminal importance for the processing of the aforementioned data.

According to Article 2 (b) of the Data Protection Directive, 'data processing' is defined as '*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*'. It follows that the definition of processing is extraordinarily broad, so that it is difficult to conceive any operation performed on personal data which would not be covered by it. It is important to note that mere storage of personal data by the providers of publicly available electronic communications services or of a public communications network constitutes 'data processing', so that simply storing data on a server or other medium is deemed to be processing, even if nothing else is being done with the data.

In addition, the relevant data protection legislation defines three distinctive categories of parties:

- ***Data subject***: the individual which is the subject of the personal data.
- ***Data controller***: a person (natural or legal) which alone or jointly with others "determines the purposes and means of the processing of personal data"[27]
- ***Data processor***: a third party who simply processes personal data on behalf of the data controller without controlling the contents or use of the data.[28]

[27] Article 2 (d) Data Protection Directive
[28] Article 2 (e) Data Protection Directive

The classification of a natural/legal person as 'data controller' or 'data processor' is of great importance for several issues, such as who shall carry the obligations appointed to the 'data controller' by the Data Protection Directive and who is to define the details of the data processing. As a rule of thumb it can be said that the data controller is liable for violations of the Data Protection legislation, while the role of the data processor is reduced[29].

Under the regime established by the Data Protection Directive, a key concept is that of the 'data subject's consent'. If the data controller obtains the data subject's consent then he/she is broadly free to process the personal data. The Directive defines 'data subject's consent' as being freely given, specific and informed.[30] It supplements this in the substantive provisions when referring to consent as being 'unambiguously' given[31]. Indeed, the definition of 'consent' in the Data Protection Directive is quite restrictive, requiring that the data subject be clearly informed in advance of what he/she is consenting to and that any processing of the data going beyond what is disclosed to him/her will be deemed not to have been consented to, meaning that it will be invalid. Particular risks arise in the online environment since there is an increased danger that the data subject might not have been fully informed or might not understand exactly what he/she is consenting to.

5.2.2 Data Protection terminology in mobile networks

As regards the field of mobile electronic communications, the term communication is of utmost importance. 'Communication[32] means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information'.

Furthermore traffic data[33] means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Such data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. Traffic data, that are needed for billing and interconnection payments may be processed until the end of the period during which the bill may lawfully be challenged or payment pursued.[34] The Working Party 29 stipulated that this should ordinarily involve a routine storage period for billing of maximum 3-6 months, with the exception of particular cases of dispute where the data may be processed for a longer period.[35] Processing of traffic data is also allowed for the purposes of marketing electronic communications

[29] Kuner, C., *European Data Privacy Law and Online Business*, Oxford University Press, 2003, p.62
[30] Article 2 (h) Data Protection Directive
[31] Article 7 (1) and 26 (1) (a) Data Protection Directive
[32] Art. 2 (d) ePrivacy Directive
[33] Art. 2 (b) ePrivacy Directive
[34] Art. 6 (2) ePrivacy Directive
[35] Art. 29 Working Party, WP 69, Opinion 1/2003 on the storage of traffic data for billing purposes (29 January 2003) available online at
http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp69_en.pdf

services or for the provision of value added services[36], if the subscriber or user to whom the data relate has given his/her consent. However any natural/legal person that already has the e-mail addresses (traffic data)[37] of its customers may use them for direct marketing of its own similar products or services, without the consent of the customer. Suffice it to say that the customer may withdraw his/her consent at any time.

Location data[38] means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. Although the ePrivacy directive does not make use of the term 'Location Based Services', article 2(g) of the Directive defines the term 'value added service' as 'any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof'. Thus we could say that a Location Based Service (LBS) is a value added service which processes location data other than traffic data for purposes other than what is necessary for the transmission of a communication or the billing thereof.

It is worth mentioning that according to the recent data retention directive[39] traffic and location data can be retained for longer periods by derogation from the aforementioned provisions of the ePrivacy directive. Specific categories of traffic and location data, as described in detail in article 5 of the data retention directive, shall be retained for periods of not less than six months and not more than two years from the date of the communication for the purpose of the investigation, detection and prosecution of serious crime. What falls under the term 'serious crime' will be determined by each Member State in its national law.

5.3 Basic Principles in Data Processing

Both EU Directives refer to basic principles for data the processing of data. These principles are intended to be good practices that data controllers should comply with in order to protect the data they hold, reflecting both their interests and those of the data subjects (Walden 2003, p.432). It should be kept in mind that the given set of principles must be applied, as such, in every case where personal data are collected and processed; for this reason, the fact that the collection of data is realised through an electronic medium, such as a mobile electronic communications network is of secondary importance. Indeed, this was one of the main goals of the legislation: to apply a sound and effective data protection framework, applied evenly across the business and industry sectors.

[36] Art. 6 (3) ePrivacy Directive
[37] Art. 29 Working Party, WP 37, Working document: Privacy on the Internet- An integrated EU Approach to On-line Data Protection. (21 November 2000) available online at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf
[38] Art. 2 (c) ePrivacy Directive
[39] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending directive 2002/58/EC, O.J. L105, pp.54-63

5.3.1 Fair and lawful processing

The first of these principles requires fair and lawful processing.[40] In determining whether any processing of personal data is 'fair' particular regard must be paid to the method by which data were obtained. For example, personal data are to be regarded as having been obtained unfairly unless, at the time of the obtaining, or very soon afterwards, the relevant data subject is provided with certain information, mainly those mentioned in article 10 of the Data Protection Directive (Carey, 2002, p.54). On the other hand, 'lawful processing' means that the data controllers should comply and uphold their legal obligations, general and specific, statutory and contractual, regarding the processing of personal data. Of particular relevance will be the laws regarding the building of a trusted relationship (especially the confidence that should exist between the data subject and the data controller), as well as article 8 of the European Convention on Human Rights (the requirement for respect for the private life of the individual).

5.3.2 Finality principle

Under the finality principle, data controllers must obtain data only for specified and legitimate purposes, and must not carry out any further processing which is incompatible with those purposes.[41] For example, a contravention of this principle would be for a company to notify the storage of customers' personal data for billing purposes, and use it additionally for marketing purposes. This principle has thus two components:

(1) The data controller must specifically inform the data subject of the purposes for which data has been collected and

(2) Once data has been properly collected, they must not be used for further purposes incompatible with the original purposes.

As regards the question whether personal data have been collected '*legitimately*', it goes without saying that it would be illegal to collect personal data without having a clear legal basis to do so. A clear violation of this principle would be the use of '*spyware*', which acts by definition without informing the user, and therefore constitutes 'a form of invisible and not legitimate processing'[42]. However the further processing of data[43] is allowed without other reasoning if the data are further processed in a way compatible with the initial specified, explicit and legitimate purposes. There are great divergences in the way the national Data Protection Authorities construe a term as '*compatible*' or '*incompatible*'. Therefore the companies shall have in mind that they must inform the data subjects about the further processing of the data, so that they can avoid the characterisation of their processing as not compatible with the initial purposes.

5.3.3 Data minimisation principle

The third principle requires a data controller to hold only personal data that are '*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or*

[40] Article 6 (a), Data Protection Directive
[41] Article 6 (b) Data Protection Directive
[42] Art. 29 Working Party, WP37, 'Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by non-EU Web-sites (30 May 2002), p.12, available at: http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf
[43] Art. 6 (1) (b). al. 2 Data Protection Directive

further processed'[44]. Data controllers are therefore obliged to store only a bare minimum of data, which suffice for the running of their services. In the same context, the design and technical devices of the data processing systems must be oriented towards collecting processing and using either no personal data or as little as possible ('data avoidance') (Holznagel and Sonntag, 2003). For this purpose, it is advised that privacy issues and in particular the processing of personal data (with the further implications regarding identity management) be taken into account at the earliest stage of the organisation of the network infrastructure ('privacy by design' – Dumortier and Goemans, 2004, p.193). However, this principle tends to be commonly disregarded by commercial entrepreneurs.

5.3.4 Data quality principle

According to the data quality principle all personal data '*shall be accurate and, where necessary, kept up to date*'[45]. The specific legislative provision creates an obligation for the data controllers to take every reasonable step to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected, are either erased or rectified. In practice, a data subject is likely to complain of a breach of this principle in cases where there has been some detriment to the individual as the result of the information being incorrect. It is therefore advised that the data controllers set up a mechanism whereby the data subjects are able to update their personal data or notify the data controller about the inaccuracies of the present information. This mechanism could be set up either within the network platform (by using the network's interface) or outside the platform (e.g. by the use of a 'hotline').

5.3.5 Conservation principle

The fifth principle stipulates that personal data shall not be kept for longer than is necessary for the purposes for which this data was collected.[46] It implies that data should be destroyed or rendered anonymous when the specified purpose for which they were collected has been achieved. On a literal interpretation of the Data Protection Directive, the processing of personal data for the purpose of anonymisation clearly falls within the scope of the Directive (since the definition of the term 'processing' is so broad that it encompasses the process of anonymisation). However, a purposive approach to the interpretation[47] would look to the object of the Directive, the protection of the individual's right of privacy, and may conclude that to impose compliance obligations in respect of the process of anonymisation would be counter, or at least neutral, in respect of achieving the Directive's achievement. This latter approach would also take into consideration the recital 26 of the Data Protection Directive, whereby '*the principles of data protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.*'

---

[44] Article 6 (c) Data Protection Directive
[45] Article 6 (d) Data Protection Directive
[46] Article 6 (e) Data Protection Directive
[47] Over the years, the European Court of Justice has gained a reputation for favouring a purposive or teleological approach to interpretation, rather than a literal approach. See for example the case *C.I.L.F.I.T. v. Ministry of Health* [Case 283/81 (1982) ECR 3415], where, at para. 20 the Court states that: "(…) every provision of Community law must be placed in its context and interpreted in the light of the provisions of Community law as a whole, regard being had to the *objectives* thereof and to its state of evolution at the date on which the provision in question is to be applied." (emphasis added)

5.3.6 Data processed in line with the rights of the data subject

The sixth principle requires processing to be carried out in accordance with the rights of the data subjects. More precisely, article 12 of the Data Protection Directive grants data subjects the right to obtain certain basic information from the data controller about the processing of their personal data. While article 12 explicitly requires only that exercise of the rights contained in subparagraph (a)[48] be '*without constraint at reasonable intervals and without excessive delay or expense*', it is generally accepted that these conditions apply to the exercise of the rights contained in sections subparagraphs (b)[49] and (c)[50] as well (Dammann and Simitis, 1997, p.199).

5.3.7 Confidentiality and security

The seventh principle addresses the issue of data security, requiring data controllers to take '*appropriate* technical and organisational measures'[51] against unauthorised or unlawful processing, and accidental loss, destruction or damage to the data. To the extent that this principle covers the security requirements and robustness of the network itself, this principle overlaps with the security and confidentiality requirements laid down in articles 4 and 5 of the e-Privacy Directive. Taken as a whole, this principle imposes a statutory obligation on data controllers to ensure that personal data are processed in a secure environment. This means that the data controllers must consider the state of technological development and the cost of the implementation of any security measures. Bearing in mind these factors, the security measures that are adopted by the data controllers must ensure a level of security that is appropriate to both the nature of data to be protected and the likely harm that would result from a breach of this principle (Carey, 2002, p.58). It follows that, the more sensitive the data, the more adverse the consequences of a security breach would be for the data subject, and therefore more stringent security requirements should be put in place. This is specially the case as regards the processing of health-related data. In any case, the data controllers should implement appropriate security measures to ensure that non-authorised personnel are not able to gain access to personal data. In addition, security precautions would suggest making back-up copies.

5.3.8 Data transfer to countries with adequate protection

Finally the last principle is the Notification to the Supervisory Authority in order to ensure the supervision of the data processing. The data controller must notify[52] the supervisory authority about the processing, mentioning among others the name of the controller, the purpose of the

---

[48] According to article 12 (a) of the Data Protection Directive, every data subject has the right to obtain from the controller "…i) confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of processing, the categories of data concerned, and the recipients to whom the data are disclosed, ii) communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, iii) knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in article 15 (1)"

[49] "[…] the data subject has the right to obtain from the controller […] as appropriate the rectification, erasure or blocking of the data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data"

[50] "[…] the data subject has the right to obtain from the controller […] notification to the third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate."

[51] Article 17 (1) Data Protection Directive

[52] Art. 18 and 19 Data Protection Directive

processing, the categories of data subjects, the categories of data processed as well as the recipients to whom the data might be disclosed. The notification must take place before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes, with limited exceptions.

5.4 Conclusion

This chapter attempted an overview of the European regulatory framework regarding the protection of privacy of the individual, in an era where his life is conditioned by the exponential use of mobile technologies. Indeed, in the dawning information society, the safeguarding of the privacy rights of the individuals becomes of seminal importance. The citizen faces several issues closely related to mobility on a daily basis, as he is confronted with questions regarding his identity and his physical location.

In a mobile world the identity of the user is questioned and issues arise with regard to the digital projection and manipulation of his identity. Furthermore, in such systems a variety of geospatial information is being processed, for various purposes such as for the provision of location based services and thus creating a perpetual feeling of being localised. Finally the physical location of the user is under question. His actual localisation is not always feasible, as digital mobility allows him to perform actions in several locations (e.g. mobile working).

The impact that the protected private sphere of the individual and his right of informational self-determination will have in answering the aforementioned questions is under constant evaluation by law and policy makers, lawyers and commercial entrepreneurs alike. Should the emergence of new technologies act as an instigator of legislative changes *vis-à-vis* the traditional and well-established notion of privacy? Or should the current legislative framework on privacy and data protection act as a barrier to the implementation of technological architectures which, according to the established doctrine regarding privacy, may pose threats to the private sphere of the individual? The fear of a dystopic Orwellian society advocates towards a firm implementation of data protection principles and the adoption of technologies that respect the privacy of the individuals, be it informational, spatial, or even virtual.

5.5 Key Terms & Glossary

This is a list of key terms and acronyms, being used in this chapter. For further explanations, please refer to the glossary in chapter 8 or the Wiki on Identity related Terms (FIDIS Wiki).

- Data Protection Directive
- Data Retention Directive
- DPA
- ePrivacy Directive
- Identifiability
- Identified person
- Identifiable person
- Legitimately
- Location Based Service (LBS)
- Spyware

6 Technologies Relating to mobile IDM

Contributor(s): Christer Anderson (KU), Leonardo Martucci (KU), Sven Wohlgemuth (ALU-Fr), Mike Radmacher (JWG), Denis Royer (JWG), Tobias Scherner (JWG), Jan Zibuschka (JWG)

6.1 Anonymity and De-Identification in Mobile Networks and Mobile Identity Management

This section studies how mobile identities could be managed in *mobile ad hoc networks*, which are networks constituted by small devices (e.g. mobile phones), where these networks offer a high degree of mobility. In this section, mobile *ad-hoc* networks have been chosen to provide an example case of a particular type of mobile network, as mobile *ad hoc* networks, to a large degree, embody the challenges and issues regarding privacy that are present in mobile networks in general. Moreover, the key concepts discussed in this document, mobility and identity, are of paramount importance in mobile *ad hoc* networks, as will be discussed below. Regarding mobility, by definition, mobile *ad hoc* networks are expected to offer high degrees of mobility, even without the aid of central infrastructures and services. Regarding identity, it is discussed in this section that the inherent properties of (true) mobile *ad hoc* networks make it possible for the participants in such networks to be anonymous by destroying their own identities, for example by constantly changing their IP and MAC addresses. It is in theory possible to reduce the mobile idem identity in mobile networks into the empty set – thus, enabling anonymous communication due to the lack of persistent identifiers in the network. However, we argue that such behaviour is harmful for the network sanity (i.e. the network is behaving in an expected manner), and that more advanced functions for managing mobile identities in mobile *ad hoc* networks are needed, and furthermore, that such solutions for uniquely identifying participants actually can be used as a foundation upon which it is possible to develop anonymity technologies. We label the fact that in order to provide practical anonymity one must posses a unique identifier as the *identity vs. anonymity paradox* in mobile *ad hoc* networks.

Section 6.1.1 introduces mobile *ad hoc* networks, and further discusses the problem of uniquely identifying participants in such networks. Section 6.1.2 discusses various security models for mobile *ad hoc* networks that could be used to enable persistent identifiers and mobile identity management in such networks. Section 6.1.3 introduces a number of strategies for enabling anonymity in mobile *ad hoc* networks by implementing anonymity technologies on top of security models allowing the usage of persistent identifiers.

6.1.1 Identification in Mobile *Ad hoc* Networks

Mobile *ad hoc* networks are described in deliverable DD3.3 “Study on Mobile Identity Management” as “*mobile platforms or nodes that can move freely and establish ephemera wireless networks without central entities to control it*”. By definition (Corson and Macker, 1999), mobile *ad hoc* networks may operate in isolation – that is, in the absence of any fixed infrastructure. Therefore, the concept of autonomous systems does not exist in mobile *ad hoc*

environments, implying that there is no entity controlling the network and providing services such as routing, security or even addressing[53].

The aforementioned lack of standardised addressing allows mobile network nodes to easily change their IP and MAC addresses, or even have multiple network interfaces (either real or virtual) with multiple identifiers. Thus, traditional identification in such environments, using network and data link information simply does not work. This might give the impression that nodes in mobile *ad hoc* network environments are naturally anonymous. However, senders and receivers can still be pinpointed and linked by observers in the network. In addition, having no persistent identities (that is, no mobile idem identities) is harmful for the network sanity in the long run, since it is not possible to identify malicious users in the network. In other words, in the absence of any form of persistent identities, mobile *ad hoc* networks are highly susceptible to Sybil attacks (Douceur, 2002), in which malicious users assume multiple identities in the network, preventing the usage of security mechanisms based on filters or trust assumptions.

Therefore, in order to provide reliable anonymous communication for network nodes in a mobile *ad hoc* network, persistent identifiers (i.e. mobile idem identities) are needed in the first place. Although anonymity and identities can be understood as opposites to each other, without identities, reliable anonymity is not achievable in mobile *ad hoc* environments. We call this situation the *identity vs. anonymity paradox*. For this reason, as will be described in the next section, most security models for mobile *ad hoc* networks, in one way or other, are based on the usage of some kinds of digital certificates.

6.1.2 Frameworks for Identification in Mobile *Ad Hoc* Networks

As described in the previous section, in order to provide security (including anonymity) mobile *ad hoc* networks need some kind of security framework that includes the ability to uniquely identify users. A number of such proposals have been published in recent years, which can be classified according to the following taxonomy. In all these groups, the user's identities could be based on, for instance, certificates, public/private key pairs or anonymous credentials:

1) Security models that assume that mobile *ad hoc* networks connect periodically (or at least occasionally) to an established infrastructure such as the Internet. Therefore, it is possible to rely on the established security infrastructure that already exists in the Internet, such as a PKI (Public Key Infrastructure). Security schemes in this group include (Karlg *et al*., 2004), for instance.

2) Security models that assume some centralised control for a certain number of devices, such as personal Certificates Authorities (CA) and repositories. They assume that one or

[53] There are no standards for IP assignment in mobile *ad hoc* networks. Recently, the Autoconf Internet Engineering Task Force (IETF) Working Group (IETF, 2006) was assigned to study, among other questions, the problem of addressing in mobile *ad hoc* networks.

more devices have a special role in the network, such as issuing certificates and publishing revocation lists, for instance. Solutions such as the Resurrecting Duckling model (Stajano and Anderson, 1999; Stajano, 2000) are based on a central device that controls the network. In Martucci, *et al*. (Martucci, *et al*. 2004), a security architecture is presented using multiple CA-like devices that control and secure a service-oriented *ad hoc* network belonging to a single entity, such as a home user or an enterprise. These solutions can operate isolated from an established infrastructure, although one or more nodes play a special role regarding security in the mobile *ad hoc* network, such as issuing certificates or building a network awareness regarding trust levels, for instance.

3) Security models that are based on threshold cryptography correspond to the third group. In this approach, a set of *ad hoc* network devices has parts of a private key that is used to issue digital certificates. As long as a sufficient part of these nodes is the network range, digital certificates can be issued. Threshold cryptography was first proposed in the context of *ad hoc* networks in Zhou and Haas (Zhou and Haas, 1999) and later improved in Luo *et al*. (Luo *et al*., 2002). How many nodes and which nodes are needed to issue a certificate is usually implementation dependent. As in the previous group, some nodes play a special role in the mobile *ad hoc* network.

4) The last group is PGP-like (Pretty Good Privacy) security models. They assume that every device has one or more public/private key pair (see FIDIS Deliverable D3.2 for more information) and that every device can issue its own certificates and distribute them in the mobile *ad hoc* network. Security often relies on the concept of web of trust. Such solutions are distributed enough to operate in complete isolation from any deployed infrastructure. Public key repositories are not allowed as part of proposed models in this group (otherwise it is not classified as part of this group). PGP-like solutions can be found in papers such as Hubaux *et al*. (Hubaux *et al*., 2001) and Capkun *et al*. (Capkun *et al*., 2003).

6.1.3 Enabling Practical Anonymity in Mobile *Ad-Hoc* Networks

Generally, in the context of mobile *ad hoc* networks, two main strategies for enabling anonymity currently exist:

1. *By replacing the standard ad hoc routing protocol with a routing protocol that enables anonymous communication (cp. Figure 7).*

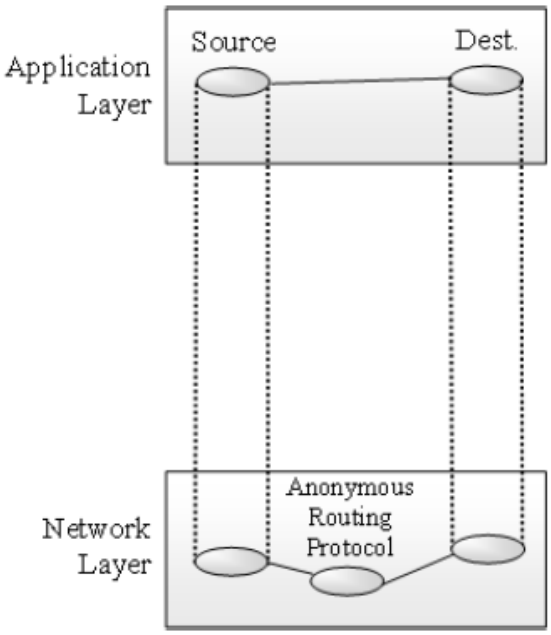


Figure 7: An anonymous routing protocol

During recent years, a number of such proposals have been published, including: ANODR (Kong and Hong, 2003), MASK (Zhang *et al*., 2005), SDAR (Boukerche *et al*., 2004), and ARM (Seys and Preneel, 2006). Most of these solutions aim to anonymise Route Request (RREQ) and Route Reply (RREP) messages during route discovery. The main advantage of this approach is that messages can be directly transmitted to the receiver using on average shorter paths in comparison with anonymous overlay networks (see below). The main disadvantage is the mere fact that the standard routing protocol is being replaced. This forces users to run another routing protocol when they want to be anonymous, and, therefore, the risk is that such solutions will end up with a small user base, and, thus, a degraded degree of anonymity according to most anonymity metrics. Another disadvantage is that the anonymity offered by this type of solutions could be betrayed in cases when a connection-oriented transport layer, such as TCP, is being used above the anonymous routing protocol.

2. *By introducing an anonymous overlay network above the ad hoc routing protocol or the transport protocol (cp. Figure 8).*

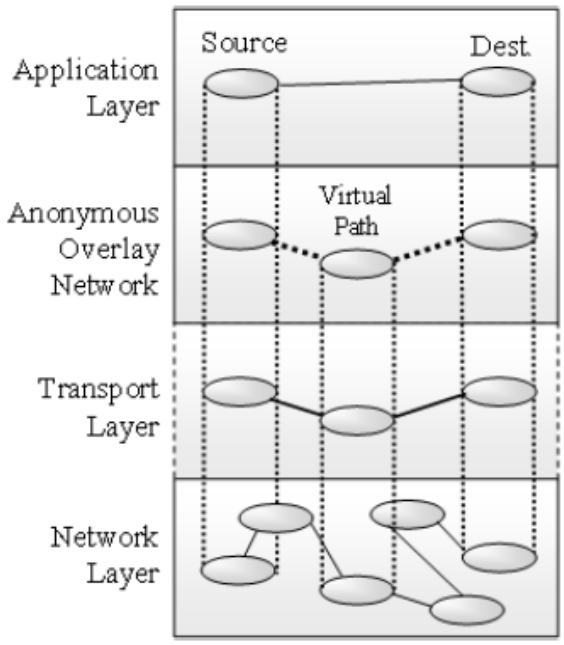


Figure 8: An anonymous overlay network

This type of solution introduces an anonymous overlay network on top of either the network layer or the transport layer. One main advantage with introducing anonymity by the means of an overlay network is flexibility; such a solution is independent of the *ad hoc* routing protocol and, furthermore, is compatible with general applications expecting services from, e.g., a reliable transport layer. One disadvantage is that the performance can be expected to be slightly worse compared to anonymous routing protocols, as messages are routed through a set of intermediary overlay nodes instead of being transmitted directly to the destination. A recent proposal belonging to this category is (Jiang *et al*., 2004), where Jiang *et al*. propose a number of adaptations to make Chaum's classical mix concept (Chaum, 1981) suitable for mobile *ad hoc* networks.

Karlstad University (Sweden) is currently working on a proposal for an anonymous overlay network called Chameleon, which adheres to the second type of solution presented above (publication under submission). The core functionalities of Chameleon are inspired by the traditional Crowds system (Reiter and Rubin, 1997) for anonymising HTTP traffic. The decision to use a Crowds-like approach was made according to a previous evaluation of peer-to-peer based anonymous overlay networks in the context of *ad hoc* networks (see Andersson *et al*., 2005 and FIDIS deliverable D3.3 for more information). Among other things, Chameleon employs end-to-end encryption between the sender and recipient, certificate-based protection against Sybil attacks, and a distributed service discovery mechanism replacing the role of the blender in Crowds. Chameleon offers sender anonymity against destinations as well as receiver and relationship anonymity against local observers for large networks. One major difference between the approach by (Jiang *et al*., 2004) is that the latter approach claims to protect against a global observer, although it is acknowledged in (Jiang *et al*., 2004) that dummy traffic could be needed in order to achieve this. For performance reasons Chameleon avoids dummy traffic, since it is commonly believed that dummy traffic and performance are orthogonal requirements in mobile ad hoc networks.

6.2 Delegation of Rights by Identity Management

In distributed information systems, delegation of rights is the process whereby a user authorises a service to access remote resources on his behalf (Gasser, M. and McDermott, E., 1990). In supply chain management, companies produce services with other companies so that they even delegate the execution of parts of their business processes to external service providers. Delegation is also used in heterogeneous environments where some devices, e.g. mobile devices, are not able to perform computationally expensive operations and so delegate them to devices with more resources, e.g. as it is the case in Grid computing (Foster, I. and Kesselman, C., 1999).

A delegation of rights is a delegation of credentials (Gasser, M. and McDermott, E., 1990; Lampson, B., Abadi, M., Burrows, M. et al, 1992; Neuman, B.C, 1993). A credential is an authorisation and binds attributes, e.g. access rights a on an object o, to a user s. Credentials are protected against forgery by cryptography. Service providers allocate access rights on his services by verifying whether a credential belongs to the requesting user (Blaze, M., Feigenbaum, J. and Lacy, J., 1996). If a credential is delegated, the attributes will be linked to this recipient (Gasser, M. and McDermott, E., 1990; Neuman, B.C, 1993; Aura, T., 1999; Welch, V., Foster, I., Kesselman, C. et al., 2004). We call such a recipient a delegatee. When a service provider receives an access request with a delegated credential, the service provider will check this credential by verifying a chain of credentials from the requesting delegatee to the issuer of this credential, usually a certification authority (CA).

While sharing credentials of type X.509 (Welch, V., Foster, I., Kesselman, C. et al., 2004), SPKI (Ellison, C., Frantz, B., Lampson, B. et al, 1999), and Kerberos (Kohl, J. and Neuman, C., 1993) with others, privacy concerns arise. Verification of these credentials traces back to the user in a chain of credentials and so his transactions become linkable. Additionally, the user will lose control of the use of his delegated credentials so that delegatees are later able to impersonate him. Credential-based identity management systems allow users to be unobservable by controlling the disclosure of personal data. This is done either by using trusted identity providers hiding the identity of a user (Erdos, M. and Cantor, S., 2002; Liberty Alliance Project, 2005) or by using anonymous credentials (Brands, S., 2000; Camenisch, J. and Lysyanskaya, A., 2001). All credentials and pseudonyms of a user are based on a secret. This secret is either his password with an identity provider or a secret cryptographic key. Showing a credential is done by proving that this user knows this secret. If a user delegates one of his credentials, he must also delegate his secret. By delegating all of his credentials and pseudonyms he reveals his identity. A delegatee is now able to link the transactions of the user, e.g. by revoking the anonymity of this user or gaining access to the profile of a user at an identity provider. He is also able to use these credential for any purpose. A delegation of credentials would not violate the user's privacy, if he trusts this delegatee. In our opinion, this trust model is not generally suitable. The challenge is to ensure privacy when delegating personal data as credentials to delegatees, which cannot be foreseen as being trustworthy.

Given below is an investigation into privacy threats when delegating personal attributes as credentials to others. This results in privacy criteria for adequate security mechanisms.

In chapter 6.2.2, we identify privacy threats while sharing capabilities with untrustworthy service providers and derive security criteria for a privacy-preserving delegation mechanism. In chapter 6.3, we evaluate credential-based identity management systems as a privacy-enhancing technology for authentication according to these privacy criteria. Finally, in chapter 6.5 we conclude with out findings and give an outlook on ongoing work.

6.2.1 Privacy and Delegation of Rights

Relating to a flow of personal information, privacy is the ability of a person to control the availability of information about and exposure of him- or herself as defined in the FIDIS Wiki. According to this definition, a person should be able to control the disclosure of his personal data. However, it does not take the use of disclosed personal data into account, which is the case when sharing credentials. The judgement of the German Federal Constitutional Court relating to the census in Germany in 1983 extends Westin's definition and takes up the use of disclosed personal data (German Federal Constitutional Court, 1983). This judgement also considers the processing of personal data. It means that every person has the right to decide about the disclosure and use of personal data. Personal data means any information concerning the personal or material circumstances of an identified or identifiable individual (German Government, 2001). It defines informational self-determination as the right of every person to decide on the disclosure and use of personal data. This right is only restricted in exceptional cases.

Based on this judgement, the following attacker model identifies privacy threats of sharing credentials with delegatees which do not seem to be trustworthy in advance. We derive criteria for privacy-preserving authentication and delegation mechanisms.

6.2.2 Attackers and Privacy Threats

Our attacker model takes two types of attackers into account: outsiders of the user's communication relationships and his communication partners. Attackers aim to trace and later to impersonate the user. We assume that an attacker cannot break cryptographic primitives and does not control the communication network.

Outsiders try to trace the user by observing his communication relationships. They also try to intercept a delegated credential in order to get information about the user by the content of this credential. Communication partners, as attackers, get personal data by means of credentials from the user within a delegation. Besides tracing a user, an untrustworthy delegatee aims to impersonate him. He tries to use a delegated credential for his own purposes. We identify the following privacy threats with a delegation of credentials:

- **Identifying a user:** Credentials express the property of personal data. If a credential contains personal data, its user can be identified when showing it.
- **Tracing a user:** Credentials are bound to a cryptographic key or a user identifier. This association is proven by showing a credential. A service provider to whom a credential has been shown or delegated is able to trace a user and link his transactions by this association.

- **Impersonation of a user contrary to the purpose of a delegation:** The process of delegation binds the particular credential to a delegatee. This delegatee is now able to use this credential for the delegation purpose but also for his own purposes, e.g. to get access to services and to get credentials linked to the own identity.
- **Re-delegation of a credential:** A delegatee shares a delegated credential of a user with other service providers. It is then possible that everyone is able to impersonate the user.

These threats show that privacy with delegation of rights results in a combination of threats concerning identification and profiling with threats concerning unauthorised access on delegated credentials.

6.2.3 Privacy Criteria for Delegation of Rights

Since attacks from outsiders can be prevented by anonymity mechanisms, e.g. mix networks (Chaum, D., 1981), and cryptography (Anderson, R., 2001), we focus on attacks by untrustworthy service providers. An essential requirement for security in distributed systems is that each participant is able to specify its own security interests and that these interests are guaranteed by the system (Rannenberg, K., Pfitzmann, A. and Müller, G., 1999). Therefore, we divide the criteria for a privacy-preserving delegation mechanism into two classes: The first class considers the interests of a user concerning observability and misuse of delegated credentials. The second class considers accountability of a user from the perspective of service providers. Our criteria also take the data protection directives 95/46/EC (European Commission, 1995) and 2002/58/EC (European Commission, 2002) of the European Commission into account.

In order to fulfil the interests of a user, a privacy-preserving delegation mechanism must fulfil the following criteria:

- **Authentication without revealing identifying data:** The statement of a credential, as well as its association with a user should be shown without revealing any identifying data to the service provider. A delegation should delegate the statement of the credential and not the identifying data.
- **Non-linkability of transactions:** Credentials should be shown and delegated with different pseudonyms of a user so that the corresponding transactions cannot be linked together.
- **Least privilege:** Service providers may request more rights that are necessary for the purpose of this collection. A user must be able to control the disclosure of his credentials so that only credentials relating to the purpose of a delegation are given to a service provider.
- **Preventing misuse of delegated credentials:** The use of a delegated credential should be bound to the purpose of the delegation. We define the purpose by the delegatee, the services or their type to which the delegatee is allowed to show the credential, the validity of a delegated credential, the allowed number of usage, and whether a recipient is allowed to re-delegate a credential. The appropriate use of a delegated credential should be guaranteed and verifiable.

- **Restricting re-delegation of a credential:** A re-delegated credential should only be valid if the user has given his consent to the re-delegation. This should be verifiable.
- **Revocation of a credential:** A user must be able to revoke a delegated credential, if the delegation purpose has finished earlier than expected, the certified statement is no longer valid, or the delegatee has been shaped up as an attacker.

The security interests of service providers relate to accountability of their users. A privacy-preserving delegation mechanism guarantees these interests, if it fulfils the following criteria:

- **Non-repudiation of using a credential:** The use of a credential should be unambiguously assigned to the one who has shown this credential. It should be possible for the end service provider to assign the use of a credential to its user. Since this user can be the delegatee or the owner of a credential, it should be verifiable whether a delegatee or a user has used this credential.
- **Revealing of identity:** The identity of a criminal user should be revealed in exceptional cases such as fraud. It should be verifiable for everyone that an exceptional case has occurred.

In the following, we investigate credential-based identity management systems with respect to these criteria.

6.3 Privacy by credential-based Identity Management

Privacy-enhancing technologies ensure anonymity by preventing an attacker from tracing the user and identifying him. Linkability based on communication data can be prevented by using anonymity mechanisms such as a mix network (Chaum, D., 1981). In order to prevent linkability on the application layer, David Chaum proposed an identity management system with unlinkable credentials (Chaum, D., 1985). In the following, we focus on credential-based identity management systems.

6.3.1 Identity Management Systems

We categorise today's identity management systems according to the use of credentials. The first kind of identity management systems uses **credentials on partial identities**. A partial identity (Clauß, S. and Köhntopp, M., 2001) represents a role of a user for a specific situation. It consists of a pseudonym and user's attributes. Examples are *iManager* (Jendricke, U. and Gerd tom Markotten, D., 2000) and *Microsoft InfoCard* (Microsoft Corporation, 2005). A CA certifies the association between a partial identity of a user and one of his pseudonyms by a credential according to X.509. All pseudonyms and credentials of a user depend on his private key. A CA has to be a Trusted Third Party (TTP) with respect to non-linkability. Additionally, transactions of a user are linkable, if using the same credential in different transactions. A user can prevent attackers from tracing him by using a credential for one partial identity only once.

Identity management systems using **credentials for browser-based attribute exchange** differ from systems using credentials on partial identities in that a trusted third party called

identity provider manages the attributes including pseudonyms of a user on his behalf. A trusted third party (TTP) issues credentials for proving the identity of a user towards service providers. Thus a TTP acts as an anonymity proxy: on the one side, the user is identifiable and traceable to the TTP whereas on the other side, this user appears with a pseudonym. The secret of a user is his password for his account at a TTP. Examples are *Liberty Alliance* (Liberty Alliance Project, 2005), *Shibboleth* (Erdos, M. and Cantor, S., 2002) and *IBM BBAE* (Pfitzmann, B. and Waidner, M., 2003). Another browser-based attribute exchange protocol is *Microsoft .NET Passport* (Microsoft Corporation, 2003). This system does not prevent their users against undesired identification and profiling. With regard to Microsoft .NET Passport review guide (Microsoft Corporation, 2003), every user has a global identifier and each service may obtain every attribute of a user.

Identity management systems of the third kind realise **anonymous credentials**. Stefan Brands (Brands, S., 2000) as well as Jan Camenisch and Anna Lysyanskaya (Camenisch, J. and Lysyanskaya, A., 2001) have developed protocols for anonymous credentials. The latter protocols are implemented by *IBM idemix* (Camenisch, J. and Herreweghen, E.V., 2002). A user is able to show a credential without revealing any identifying attributes. This is done by using zero-knowledge proofs. A credential can be shown be using different pseudonyms so that these transactions seem to be independent. Even a CA cannot recognise a user if he shows a credential issued by this CA with a different pseudonym. Furthermore, a user can decide which attributes of a credential are revealed in a proof. From the service providers' view, *idemix* supports accountability so that the identity of a user can be revealed by a third party under certain conditions. In order to prevent users from sharing their credentials, *idemix* binds all pseudonyms and credentials of a user on his secret key and uses alternatively two non-transferability mechanisms: PKI-based non-transferability and all-or-nothing transferability.

6.3.2 Delegation of Rights and Identity Management Systems

Identity management systems with anonymous credentials and credentials for browser-based attribute exchange support non-linkability by controlling the disclosure of personal data, the latter under the condition of an involved TTP relating to privacy. Identity management systems are not suitable to protect personal data once they have been revealed. This is exactly the case when sharing credentials.

Concerning browser-based attribute exchange, *Liberty Alliance Phase 2* considers in their specification (Liberty Alliance Project, 2005) an approach for delegation of rights. But their approach contradicts with their trust model with respect to privacy. They assume a delegatee to be the attacker and a TTP hides the identity of the user by encrypting it with the public key of the end service provider. This end service is thereby able to encrypt it and identify the user. Contrary to this trust model, the specification (Liberty Alliance Project, 2005) assumes that every service provider wants to share their profiles about their users.

Concerning anonymous credentials, *idemix* assumes that the cryptographic key on which all credentials are based on is kept secret. Sharing this secret key with a delegatee would infringe this assumption. This delegatee is able to link the transactions of a user with other service

providers by revealing user's identity. Additionally, this user would lose control of his credentials since the delegatee would be able to impersonate the user and thereby use all credentials of this user. He is able to get credentials and establish pseudonyms for own purposes but on behalf of the user.

Consequently, if a user delegates credentials to untrustworthy delegatees, he will not have privacy at all. A privacy-preserving delegation mechanism should introduce an alternative for sharing user's secret and ensure the use of delegated credentials according to the security interests of this user. We will use *idemix* and protect delegated, anonymous credentials from misuse and tracing back to the user by an access control which focuses on the identified privacy criteria.

6.4 State of the Art Application Scenario: The PRIME LBS Prototype

One example of a state-of-the-art privacy-respecting application is developed by T-Mobile in cooperation with University of Frankfurt as part of the PRIME project[54]. For T-Mobile, the prototype leads to new insights into how privacy enhanced identity management can be introduced into a mobile commerce (m-commerce) scenario without restricting the business models. An idea on how privacy enhancing services can be deployed within a telecommunication environment, especially as a standardised IDM management system, can leverage new and efficient business models in such a scenario.

In this setting, several challenges and opportunities for privacy enhancing technologies appear - the system should:

- Control the flow of dynamic personal information, such as location or service usage
- Determine who has received personal information for which purpose
- Delegate handling of context-based personal information
- Hide specifics of service usage from mobile operator
- Anonymise user towards service provider
- Provide a unique interface for all supported services
- Have a substantial initial installed user base for profitable, privacy-friendly LBSs

The prototype demonstrates how the user is given extended control of his personal information, but is still able to use a real mobile m-commerce application using features of the PRIME suite, including communication, authentication, authorisation, policy management, data track and automatic handling of personal information.

[54] For further information, please refer to the PRIME project homepage: www.prime-project.eu.org.

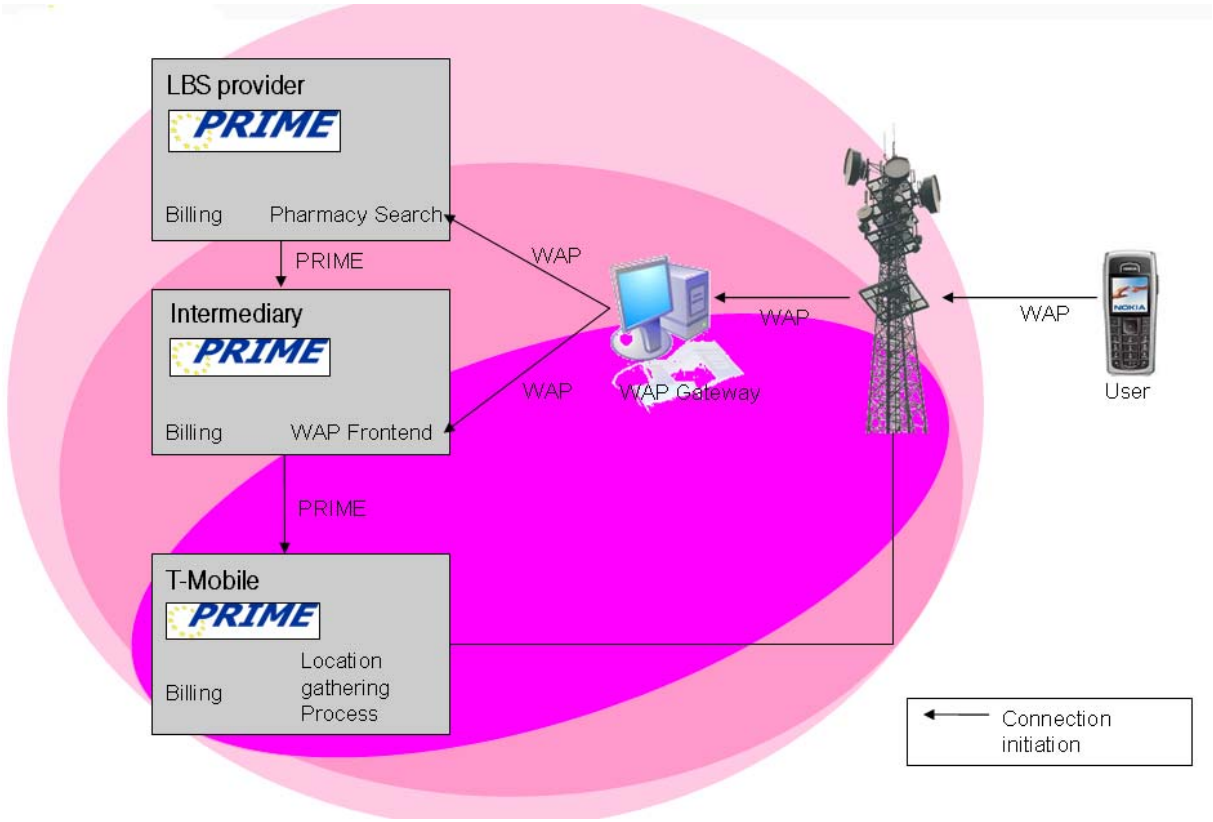


Figure 9: Prototype Version 1 - Architecture Overview

A first prototype version has already been finished: a mobile pharmacy search using Wireless Application Protocol (WAP). The usage of this widely deployed protocol enables T-Mobile to reach a maximum footprint for upcoming privacy-enhanced products.

In this scenario (cp. Figure 9) we have three different parties beside the mobile subscriber. The mobile operator offers the communication infrastructure, locates the user and takes care of the billing process. The location intermediary cleanly separates the spheres of mobile operator and service provider, which in our case, is the provider of pharmacy locations. The LBS application service provider maintains a database with pharmacies and their respective locations. When a user requests information about the closest pharmacy to his position, his location is retrieved and the pharmacy database is queried. Then a list with the closest few pharmacies is returned to the user.

A next version of the prototype will be a push service, and deploy the PRIME user side on a mobile phone to reach even stronger privacy guarantees. In addition to (anonymous) PRIME credentials, the (anonymous) PRIME communication channels and dynamic personal information facilities will be employed to provide for a solid protection of users' privacy.

6.5 Conclusion and Outlook

This chapter describes the interplay of privacy with the delegation of rights by means of credentials, extending the concepts described in FIDIS deliverable D3.3. We discovered that

such a delegation with today's identity management systems requires a delegation of a user's secret which means sharing personal attributes and credentials with others. It follows that a user will lose control of his identity and consequently of his privacy.

Freiburg University will extend *idemix* in order to protect delegated credentials from misuse and tracing back to the user by an access control on delegated, anonymous credentials which focuses on the privacy interests of the user. We will further compare our approach with trust-building measures such as obligations (Hilty, M., Basin, D. and Pretschner, A., 2005), user-controlled access control on disclosed attributes at service's side (Hohl, A. and Zugenmaier, A., 2005) and a verifiable reporting mechanism relating to the enforcement of privacy policies (Karjoth, G., Schunter, M. and Waidner, M., 2003).

Furthermore, the PRIME application prototype is introduced, as a state of the art application scenario for privacy-respecting mobile applications

6.6 Key Terms & Glossary

This is list of key terms and acronyms, being used in this chapter. For further explanations, please refer to the glossary in chapter 8 or the Wiki on Identity related Terms (FIDIS Wiki).

- Anonymous Credentials
- Application Layer
- Certification Authority (CA)
- Credentials
- Linkability
- Mix Network
- Partial Identity
- Public Key Infrastructure (PKI)
- Trusted Third Party (TTP)
- X.509

7 Conclusion and Outlook

Contributor(s): Denis Royer (JWG), Layla Nassary Zadeh (JWG)

7.1 Conclusion

The objective of this study is the identification, the description, and the application of the topics and elements in the fields of "*mobility and identity*", exploring some of the essential concepts, fundamental to the work of Work Package 11. Starting from the work of FIDIS deliverable D3.3, not only technological aspects are included, but also socio-cultural, legal, and economical aspects are taken into consideration for this study and for the work of FIDIS Work Package 11:

- Starting with the socio-cultural aspect, this includes the term mobile identity, which is mainly used as a mobile idem identity type, meaning that in the process of identity building, people reflect about the mobile idem identities (which are third person perspectives) in order to constantly (re-)develop a sense of self (the ipse identity or the first person perspective).
- Furthermore, an overview of the European regulatory framework regarding the protection of privacy of the individual is given, presenting the questions of localisation and privacy protection of persons in mobile service / LBS scenarios.
- Last but not least, GSM and other communicational technologies are described as an example for the application of mobility and identity in the field of technology.

Due to the ongoing evolution of the presented concepts of "mobility and identity" and "mobile identity", this study cannot be exhaustive. It represents the foundation towards a taxonomy of mobility and identity, which could be used as a tool facilitate the circulation and the creation of new ideas related to this topic. Moreover it should allow to identify further overlaps as well as future research topics for FIDIS and especially for Work Package 11 (cp. chapter 7.2). Finally, the researched concepts and terminology is added to the FIDIS concept of identity[55] or the "*FIDIS Wiki on Identity related Terms*", in order to broaden the horizon of classical identity concepts, presented in other FIDIS deliverables.

[55] For details, please refer to the deliverables of FIDIS Work Package 2. These are available for download at www.fidis.net/del_fidis.0.html

7.2 Outlook on WP11 Deliverables

7.2.1 D11.2: Mobility and Location Based Services (LBS)

LBS are essentially information services that exploit the ability of technology to know where things are located, and to modify the information it presents accordingly (cp. Figure 10). In D11.2 we want to take a closer look at the topic of "Mobility and Location Based Services". A major task of this deliverable will be the evaluation of Location Based Services (LBS) from the perspective of technology, profiling, identification, and privacy, starting with an overview of "Location Based Services" (LBS) on the basis of typical Use Cases. Questions that need to be answered as a next step are: What is the Connection between LBS and Mobile Identity? What is the influence of Mobile Identity on LBS? Furthermore, we are going to present the different perspectives, especially of the other work packages, on LBS.

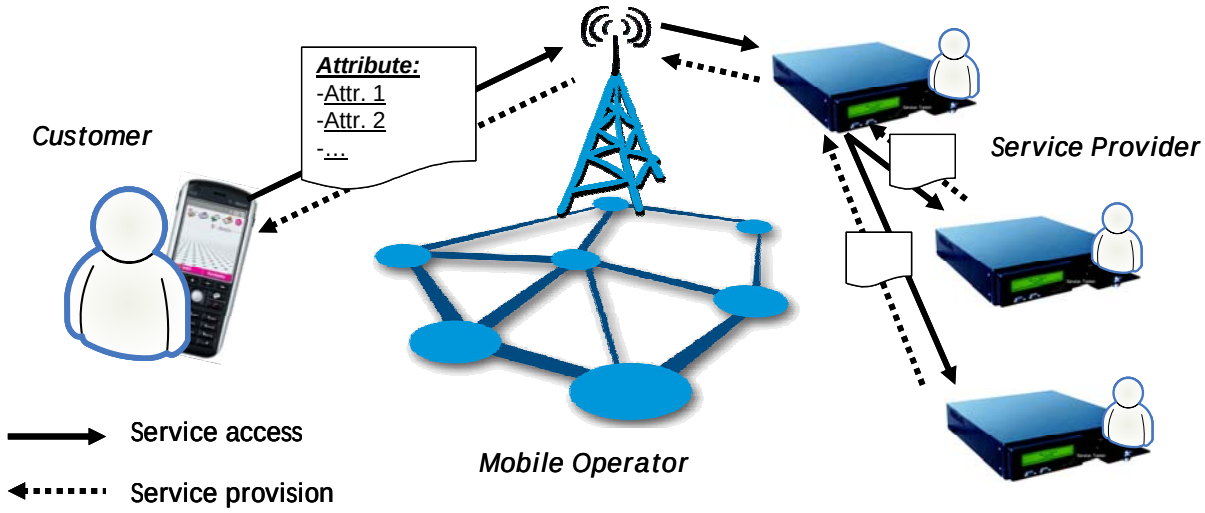


Figure 10: Mobile services and the transfer of partial identities.

7.2.2 D11.3: Economic aspects of mobility and identity

In this study, the economic evaluation of mobile identity management systems and their influences on our everyday life will be the central topic. New business models, business processes, and mobile services will be the key factors that will be analysed. Also, the market acceptance and the general mechanisms for the diffusion of new technologies into an emerging market will be taken into consideration.

7.2.3 D11.5: Study on private and public access to identifiable location data

Furthermore, a study on "Private and public access to identifiable location data" will address the (lack of) legal framework relating to the use of identifiable location data by public parties (law enforcement) and private parties (employers). Not only various forms of mobile ID systems will be taken into account and mapped, but also the outcome of these systems in the form of the resulting location data. The study will analyse to what extent the police have access to the location data in the various systems, based on the powers they have. A further interesting question is whether private parties, who lack the powers the police have, such as employers, have any legal ground to access these systems. This question is of importance as employers increasingly make use of positioning systems in order to monitor their employees,

or to manage them on the basis of location data gathered through these systems. Not only the legitimacy but also the technical specifications of monitoring and positioning systems will be taken into account. More specifically the question whether third party access to location data is desirable in view of privacy issues and 'a right to anonymity' will be addressed. These rights will be evaluated in view of the interests of the third party as well as the public interest. Not only the legal powers to access data and the legal guarantees against misuse of these data will be addressed, but the technical specifications of mobile id systems that can influence access and use of data will be taken into account. The main questions to be addressed are:

- What guarantees (legal as well as technical) (need to) exist in order to counterbalance the empowerment of employers caused by monitoring and positioning systems and the (mis)use of location data gathered through these systems?
- Which conditions apply to requests for location data from LBS providers?
- Which powers exist for the police to order LBS providers to preserve ('freeze') location data?
- Is there a requirement for data retention?

The legal framework will be assessed from a number of EU jurisdictions, (for example the Netherlands, Belgium, Germany, France, the UK), and possibly from US law. Because of the different approaches to privacy and law enforcement, as well as in employment law, this will make an interesting comparison.

7.2.4 D11.6: Survey on Mobile Identity Management (& LBS)

Another task will be a survey conducted by Work Package 11 by asking professionals and everyday users about their behaviours and usage patterns with regard to mobile IMS and LBS. One goal will be to determine the willingness of the users to pay for such services. Furthermore, by conducting a second survey on the same sample, which explains the possible threads of LBS and the need for mobile IMS (see D11.2 and D11.3), the awareness of the users with regard to LBS and mobile IMS can be analysed.

8 Glossary

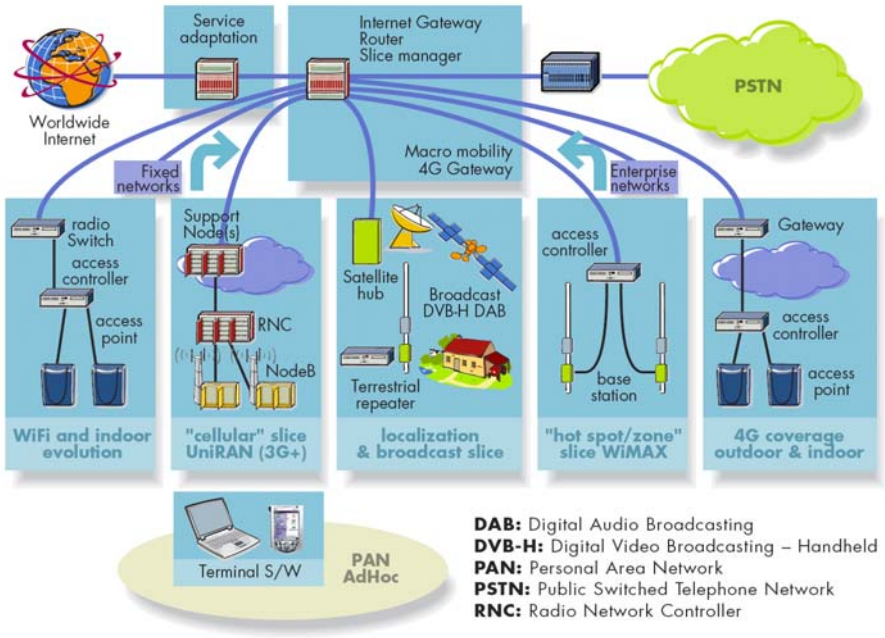
This section contains the general glossary and the definition of the terminology used in this document. All terms can also be found in the general FIDIS Wiki on Identity Management at: http://internal.fidis.net/fidis_wiki.0.html.

3G (or 3-G):

3G is short for third-generation mobile telephone technology. The services associated with 3G provide the ability to transfer both voice data (a telephone call) and non-voice data (such as downloading information, exchanging email, and instant messaging). Originally, 3G was supposed to be a single, unified, worldwide standard, but in practice, the 3G world has been split into four different fractions: UMTS (W-CDMA), CDMA 2000, TD-SCDMA, Wideband CDMA

4G (or 4-G):

Fourth Generation (4G) networks focus on mobile communication and are seen to be successors of the Third Generation (3G) wireless access technologies that are in use today. 4G networks are sometimes referred to as "3G and beyond" networks, too. Besides new radio based wireless access technologies with higher bandwidths and more sophisticated Quality of Service functionalities, 4G Networks are planned to provide pervasive computing concepts for the user. Pervasive networks will be the basis for pervasive computing where the environment of the user consists of a wide range of dedicated and communicating devices collaborating to provide services that adapt to the current situation of the user.



Essentially, 4G networks will integrate a wide range of different wireless technologies, including existing 3G networks (e.g. UMTS or WiMAX) as well as novel 4G wireless communication, in order to provide continuous coverage in all situations by relying on

different access technologies. This explicitly includes short range radio, to be used for the communication between local devices and mesh-networking approaches, as well as long range communication for broadband linkup to the Internet.

Anonymous Credentials:

In the widest sense, a credential is a piece of information attesting to the truth of certain stated facts. Credentials are used in the process of authentication, and in this context are based on the following technologies: Biometrics, digital certificates, smart cards, passwords etc. By using anonymous credentials, organisations know the users only by pseudonyms. Different pseudonyms of the same user cannot be linked. Yet, an organisation can issue a credential to a pseudonym, and the corresponding user can prove possession of this credential to another organisation (who knows her by a different pseudonym), without revealing anything more than the fact that she owns such a credential.

Application Layer:

The application layer is the seventh level of the seven-layer OSI model. It interfaces directly to and performs common application services for the application processes; it also issues requests to the presentation layer.

The common application layer services provide semantic conversion between associated application processes. Examples of common application services of general interest include the virtual file, virtual terminal, and job transfer and manipulation protocols.

Biometrics:

Biometrics is the application of mathematical and statistical methods to the study of biology.

Human characteristics which are useful in biometrics are 1. Physical aspects as fingerprints, hands scans, eye patterns, ear patterns, facial features and DNA and 2. Behavioural characteristics like signatures, voice and keystroke dynamics (information derived from Hes R. *et al.* At face Value on biometrical identification and privacy. Achtergrondstudies and verkenningen 15 Registratiekamer The Hague, 1999, pp.19-24.)

Biometrics is referred to as a number of methods to authenticate persons using physical features (such as fingerprints) or behaviour (such as voice recognition).

CCTV:

Closed Circuit Television.

Cell:

Cells are base stations to cover a geographic area. (Information derived from PC Magazine (http://www.pcmag.com/encyclopedia_term/0,2542,t=cellphone&i=39505,00.asp).

In a cellular mobile phone network, a cell is referred to as a base station to cover a certain geographic area.

Cell-phone:

Cellular telephone. The first ubiquitous wireless telephone. Originally analogue, all new cellular systems are digital, which has enabled the cell-phone to turn into a smart phone that has access to the Internet. Digital cell-phone systems are also offered in the PCS band, which is radio spectrum that was auctioned off by the U.S. government in the mid-1990s. Introduced in the mid 1980s, cell-phone sales exploded worldwide in the 1990s as a consequence of the success of the GSM standard.

Certification Authority (CA):

A certification authority (CA) is an entity which issues digital certificates (credentials) for use by other parties. Users trust a CA that it certifies statements about their users with respect to their certification policy. So, a CA is an example for a Trusted Third Party (TTP).

Credentials:

In the widest sense, a credential is a piece of information attesting to the truth of certain stated facts. Credentials are used in the process of authentication. In this context are based on the following technologies: Biometrics, digital certificates, smart cards, passwords etc.

Data Protection Directive:

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L281, 23.11.1995, p. 0031-0050.

Data Retention Directive:

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending directive 2002/58/EC, O.J. L105, pp.54-63

Digital Divide:

The digital divide in contemporary societies is based on the broader disconnections of certain groups from IT hardware *and* the growing use of automated surveillance and information systems to digitally red-line their life chances within automated regimes of service provision (Jupp, 2001). (From Graham and Wood **Digitizing surveillance: categorization, space, inequality.** Critical Social Policy (2003), pp.23-22.)

Digital identity:

Digital identity denotes all those subject-related data that can be stored and interlinked by a technology-based application. The subsets of the digital identity are digital partial identities (= partial digital identities) which represent the subject in a specific context. A digital identity is, in a mobile network context, cooperatively provided by the mobile network operator and the mobile subscriber. It is constituted by idem identity and ipse identity aspects.

Digital identity according to Saärenpaä: “a message which is received about a person through digital information either as such or in combination with other information of that person (characteristics, habits)” (Saärenpaä *The constitutional state and digital*

identity, Paper available on the website of the 2002 World Congress for Informatics and Law II Spain September 23rd–27th).

Data Protection Authorities (DPA):

Data Protection Authorities or else Supervisory authorities for the protection of data are one or more public authorities in each Member State that are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to the Data Protection Directive. These Authorities shall act with complete independence in exercising the functions entrusted to them. Every Authority shall have investigative powers, effective powers of intervention as well as the power to engage in legal proceedings, where the national provisions adopted pursuant to the Data Protection Directive have been violated or to bring these violations to the attention of the judicial authorities. (Art. 28 Data Protection Directive)

ePrivacy Directive:

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. L201, 31.07.2002, p. 0037-0047

Geoslavery:

'the dangers of continuous real time control through extensive use of locational data' (Dobson and Fisher, 2003).

Global System for Mobile Communications (GSM):

GSM (Global System for Mobile Communications) is the most popular standard for mobile phones in the world. GSM phones are used by over a billion people across more than 200 countries. The ubiquity of the GSM standard makes international roaming very common with "roaming agreements" between mobile phone operators. GSM differs significantly from its predecessors in that both signalling and speech channels are digital, which means that it is seen as a *second generation (2G)* mobile phone system. This fact has also meant that data communication was built into the system from very early on. GSM is an open standard which is developed by the 3rd Generation Partnership Project (3GPP).

GSM:

See Global System for Mobile Communications

Horizontal social mobility:

'transition of an individual or social object from one social group to another situated on the same level', while vertical social mobility' (Sorokin P; *Social and Cultural Mobility* 1959)

Idem identity:

Type of identity that establishes sameness, specifying an individual as 'the same person'. This type of identity presumes a third person perspective, indicates objectification and categorisation. However, it also concerns the continuity (samenness) of the first person perspective. Paul Ricoeur, *Oneself as another*, Chicago: Chicago University Press 1992. See deliverable 7.4, section 3.4.2.2 for further references.

Identifiability:

Identifiability is the possibility of being individualised within a set of subjects, the identifiability set (PRIME-project, D14.1.a)

Identifiable person:

Identified person is a person the identity of which has been corroborated (based on the definition of 'identified entity', MODINIS-Project).

Identified person:

An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Art. 2 (a) Data Protection Directive)

Identity management:

"The operations performed to support the lifecycle of the digital identity". (Roussos *et al*. 2003)

Idiosyncrasies:

A peculiarity of physical or mental constitution or temperament. Also a characteristic belonging to, and distinguishing, an individual; characteristic susceptibility; idiocrasy; eccentricity.

iManager:

iManager is an identity manager for a mobile user in order to support him to communicate securely, to manage his partial identities, and consequently to protect his privacy. iManager has been developed at the University of Freiburg (Prof. Müller), Germany. It is a client side identity manager, which means that it is part of the user's mobile device, and can be classified as a type 3 IMS (cp. FIDIS deliverables 3.1 & D3.3).

Information and Communication Technology (ICT):

ICT is a technical term circumscribing networking infrastructure, systems and applications facilitating communication (voice and data) and processing of information (including collection, storage and transport).

Ipse Identity:

The ipse identity is the sense of self of a human person. It presumes a first person perspective and resists complete determination. Ipse identity is not categorical or static but underdetermined and dynamic. The continuous reconstruction of the sense of self builds on the relational constitution of the self. According to Ricoeur the sense of self has a narrative structure: it consists of the autobiography we tacitly or explicitly reconstruct of our own life, fitting actions and other events into a coherent story that we recognise as our own life's story. Paul Ricoeur, *Oneself as another*, Chicago: Chicago University Press 1992. See deliverable 7.4, section 3.4.2.2 for further references.

Legitimately:

In compliance with the existing European legal framework.

Linear 4G vision versus **Concurrent (WLAN) 4G vision (cp. 4-G)**:

The linear scenario for 4G refers to '*an extrapolation from current trends towards increasing the bandwidth delivered by mobile communications and envisages the widespread availability of 4G mobile communications some time around 2010. This scenario projects forward the view of mobile communications as having evolved through a series of successive generations, a view that it is implicit in the term "fourth generation"*.' (IPTS Project report. (2004) "The Future of Mobile Communications in the EU: Assessing the potential of 4G", p.11).

The Concurrent 4G Vision refers to '*the possibly disruptive impact of the emergence of public wireless local area network (WLAN) access. To a limited extent WLAN access is already available today, and plans are afoot to deploy large numbers of so-called "hot-spots" offering semi-mobile Internet access. This approach enables a high bandwidth service to be offered at relatively low cost in specific locations where usage is likely to be concentrated*' (IPTS Project report. (2004) "The Future of Mobile Communications in the EU: Assessing the potential of 4G", p.11).

Linkability:

Linkability describes the extent to which a given data set allows one to establish identity between two or more pseudonyms. It is an important measure for privacy enhancing technology because it is a measure of the degree of loss of anonymity in a context.

Linkability is defined for 2 or more pseudonyms in relation to a data set and an anonymity set. It is a measure of how much the data allows one to establish identity between two or more items in the context. The quantity increases the smaller the group of pseudonyms that are identified with a particular pseudonym (or group of pseudonyms) in a particular context. For example if it is known that a pseudonym contained in a cookie corresponds to a social security number in a database then maximal linkability has occurred in this context.

Location:

A particular place in physical space.

Location-based service (LBS) - general:

Location-based services (LBS) are services, provided in a mobile network to the subscriber's mobile device, based on their current geographical location. This position can be known by user entry or a by other locational systems, such as GPS receiver. Most often the term implies the use of a radiolocation function built into the cell network or handset that uses triangulation between the known geographic coordinates of the base stations through which the communication takes place.

Location-based service (LBS) - legal:

The European Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) does not make use of the term 'Location Based Services'. However, article 2(g) of the Directive defines the term 'value added service' as '*any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof*'. We could say that a Location Based Service is a value added service which processes location data other than traffic data for purposes other than what is necessary for the transmission of a communication or the billing thereof.

Location information:

The physical or logical location of the materials being described.

MAC Address:

In computer networking a Media Access Control address (MAC address) is a unique identifier attached to most forms of networking equipment.

Mix Network:

A mix network guarantees an effective form of anonymisation on the Internet and consists of several mix nodes. A mix is a proxy computer within a mix network that collects the encoded messages sent by the various users of a communications network. Subsequently, it changes the codes of these messages and their order for the transmission to next mix in line. There, this procedure takes place anew. The last mix of the route finally identifies the actual receiver and delivers the encoded message to them. A mix network works reliably even when only one mix is working reliably.

Mobile identity:

An idem identity type, based on a message or a set of (linked) messages derived from mobile computing devices, constituting claims about the mobility, the location or other characteristics which are assumed to represent a data subject.

A mobile identity in the wide sense is a partial identity which is connected to the mobility of the subject itself, including location data. The mobile identity may be addressable by the mobile ID. Typical settings for mobile identities comprise the use of mobile phones, the use of mobile tokens which store identity data, or the use of RFIDs (Radio Frequency IDs). Furthermore the mobility of a subject may be observed by others including the deployment of tracking mechanisms with respect to biometric properties, e.g., by a comprehensive video surveillance. This additionally may be understood as a mobile identity (FIDIS deliverable D3.3).

Mobile identity management (m-IDM):

Mobile identity management is a special case of identity management where location data is taken into account. It comprises both the perspective of the subject whose partial identities are concerned, e.g., offering mechanisms to decide when and what location data is used and transmitted to whom and the perspective of the mobile identity (management) provider who operates the system and may process the subject's data. (FIDIS deliverable D3.3).

Mobility:

Mobility is the ability and willingness to move or change. (wikipedia)

Omniperception:

'Omniperception is the aspiration to have knowledge over all people' (Lyon D., *Surveillance society. Monitoring everyday life,* 2001, pp.124).

P3P

See Platform for Privacy Preferences Project.

Platform for Privacy Preferences Project:

P3P has been developed by the World Wide Web Consortium (W3C) and is an industry standard designed to help users gain more control over the disclosure and use of their personal information on Internet sites they visit.

Partial Identity:

Each identity of a subject can comprise many partial identities of which each represents the subject in a specific context or role. Partial identities are subsets of attributes of a complete identity. On a technical level, these attributes are data.

Privacy Enhanced Technologies (PET):

'T*he concept of Privacy Enhancing Technologies (PETs) aims at organising/engineering the design of information and communication systems and technologies with a view to minimising the collection and use of personal data and hindering any unlawful forms of processing by, for instance, making it technically impossible for unauthorised persons to access personal data, so as to prevent the possible destruction, alteration or disclosure of these data. The practical implementation of this concept requires organisational as well as technical solutions.*' (information derived from the technical workshop on Privacy-Enhancing Technologies 4 July 2003, http://europa.eu.int/comm/justice_home/fsj/privacy/docs/lawreport/pet/200304-pet-outcome_en.pdf)

Public Key Infrastructure (PKI):

PKI (Public Key Infrastructure): The architecture, organisation, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. The main ability of a PKI is to administer certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Reachability Management:

Computer and communication technology should be able to give callees more options to decide whether a call was welcome, and to protect themselves from unwelcome calls. It should also give callers more options to show the importance and urgency of their calls. Additional features allowed users to specify security features for their calls.

Reachability management offers callees the possibility to specify the circumstances, under which they are willing to receive a call. This specification, together with the information callers provide during the call request, is the basis for the decision whether the callee is immediately notified of the call, e.g. whether the telephone bell rings. Reachability management was sometimes described as a "Secretary for those who cannot afford a real one".

Right to privacy:

'The freedom from unreasonable constraints on the construction of one's own identity'. (Agre and Rotenberg, 2001).

SIM:

See Subscriber Identity Module.

Smartphone:

Mobile phone equipped with a runtime environment and / or operating system that allows for installation and running of additional applications. Many of today's smartphones include the functionality of a PDA.

Social mobility:

Changes in the socio economical status (SES). Social mobility can be the result of '(1) structural changes in the working population, new positions become available or some positions experience a lack of people (there can be a demographical cause) or (2) efforts of individuals, to generate a certain position (e.g. educational level – importance of status gaining processes)' (J. Vincke. Classical Introduction in Sociology, 1998 – translation from Dutch. Original title; Klassieke inleiding in de sociologie).

Spyware:

The term spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Subscriber Identity Module:

A subscriber identity module (SIM) is a smart card securely storing the key identifying a mobile subscriber. SIMs are most widely used in GSM systems, but a compatible module is also used for UMTS UEs (USIM) and IDEN phones. The card also contains storage space for text messages and a phone book. (FIDIS deliverable D3.3).

TCP/IP reference model:

The TCP/IP reference model is the set of communication protocols that implement the protocol stack on which the Internet runs. It is named after the two most important protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). TCP is a reliable, connection-oriented protocol for exchanging data packets between applications. IP is a data-oriented protocol used for communicating data across a packet-switched internetwork.

Trusted Third Party (TTP):

A trusted third party (TTP) is an entity which facilitates interactions between two parties who both trust the third party; they use this trust to secure their own interactions. TTPs are common in cryptographic protocols, for example, a certificate authority (CA).

Vertical Social Mobility:

'*transitions of people from one social stratum to one higher or lower in the social scale*' (Sorokin P., *Social and Cultural Mobility*,1959)

Virtual Private Network:

This describes technical solutions providing for confidential end-to-end communication or data transfer using non trusted or publicly available network infrastructure such as the internet or mobile communication networks. For this purpose usually the confidential data is encrypted. The encrypted end-to-end communication also is referred to as VPN tunnel. The figure below shows an example of a VPN, connecting two private networks over the Internet.

VPN:

See Virtual Private Network.

VPN tunnel:

See Virtual Private Network.

Wearables:

Computer technology, being suitable for wear or able to be worn. Commonly, wearable computers are usually either integrated into the user's clothing or can be attached to the body through some other means, like a wristband. They may also be integrated into everyday objects that are constantly worn on the body, like a wrist watch or a hands-free cell phone. A wearable computers differs from a PDAs, which are designed for hand-held use, although the distinction can sometimes be a blurry.

X.509:

X.509 is an ITU-T standard for public key infrastructure (PKI). X.509 specifies, amongst other things, standard formats for public key certificates and a certification path validation algorithm.

9 Bibliography

Advirsson A., *On the Pre history of the Panoptic Sort: mobility in market research*, Wood D. (ed.), *Surveillance and Society*, vol. 1, number 4, winter 03/04, pp.456 – 474. Free peer to peer electronical journal available at http://www.surveillance-and-society.org.

Andersson, C., Martucci, L., Fischer-Hübner, S., *Requirements for Privacy-Enhancements for Mobile Ad Hoc Networks*, in Cremers, A. B., Manthey, R., Martini, P. Steinhage, V. (eds.), 3*rd German Workshop on Ad Hoc Networks (WMAN 2005), Proceedings of INFORMATIK 2005 - Informatik LIVE! Band 2*, volume 68 of *LNI*, pp.344–348. GI, 19th–22nd Sep 2005.

Bauer, M., Meints, M., Hansen, M. (eds.), 'D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems', FIDIS Deliverable WP 3, 2005.

Beller, M., Leerssen, J., *Identity*, Imagology. A Handbook on the literary representation of national characters, 2001.

(Note: the handbook should be published in 2006. Some articles are available at the Handbook's part of the IMAGE website www.cf.hum.uva.nl/images/dtory.identity.pdf).

Bennet, C.J., Crowe, L., *Location Based Services and the Surveillance of Mobility: an analysis of privacy risks in Canada*, A report to the Office of the Privacy Commissioner of Canada under the 2004 – 2005 Contributions Programs, June 2005 p. 44.

Bennet, C.,Regan, P., *Editorial. Surveillance and mobilities*, Wood D. (ed.), Surveillance and Society, vol. 1 number 4, winter 03/04, pp.449 – 455. Free peer to peer electronical journal available at http://www.surveillance-and-society.org.

Boukerche, A., El-Khatib, K., Xu, L., Korba, L., *SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks*, in: *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04)*, pp.618 – 624, 2004.

Cameron, K., *Laws of Identity*, version of 5/12/2005. See at www.identityblog.com.

Capkun, S., Hubaux, J. P., Buttyán, L., *Mobility Helps Security in Ad Hoc Networks*, in: *Proc. 4th ACM Symposium on Mobile Ad Hoc Networking and Computing - MobiHoc'03*, Long Beach, CA, USA, Jun. 2003, pp.46-56.

Castells, M., The Power of Identity: *The Information Age economics, society and culture volume 2*, Blackwell Publications Cornwall UK, 1997, p. 537.

Castells, M., *The Rise of the Network Society*, Blackwell Publications New York; 1996, p. 412.

Chaum, D., *Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms*, Communication of the ACM, 24(2): pp.84–88, Feb 1981.

Clarke R., *Wireless Transmission and Mobile Technologies*, 2003 See at www.anu.edu.au/people/Roger.Clarke/EC/WMT.html.

Corson, M. S., Macker, J., *Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*. RFC-2501, Jan 1999. See http://www.ietf.org/rfc/rfc2501.txt.

Carey, P., *E-Privacy and Online Data Protection*, Butterworths, 2002.

Dammann, U., Simitis, Sp., *EG-Datenschutzrichtlinie*, Nomos Verlagsgesellschaft, 1997.

Elias N., *Was ist Soziologie? Aula Boeken 462. Translated in Dutch by Goudsblom J., Vollers J.*, Junventa Verlag, 1970, p. 271.

Douceur, J. R., *The Sybil Attack*. In Druschel P., Kaashoek, F., and Rowstron, A., (eds.), *Peer-to-Peer Systems: Proceedings of the 1st International Peer-to-Peer Systems Workshop (IPTPS)*, volume 2429, pages 251–260. Springer-Verlag, 7th–8th Mar 2002.

Dooley, D., *Social Research Methods*, Prentice Hall Inc. College Div., Third Edition, 1994, p. 387.

Müller, G., Wohlgemuth, S., (eds.), *Deliverable 3.3: Study on mobile identity management*, FIDIS Work Package 3, 2005, p. 90.

Fortunati, L., *The mobile phone an identity on the move*, Personal and Ubiquitous Computing, Springer Verlag London, Surrey, vol. 5, 2001 pp.85–98.

Geser, H., *Towards a sociology of the mobile phone*, Online Publications social institute of the University of Zurich, release 3.0. 2004, p. 47. Available at http://socio.ch/mobile/t_geser1.htm

GSM Association, GSM Statistics www.gsmworld.com/news/statistics/index.shtml, visited2006-05-06, 2006.

Harper, Director Stempec Project, *Report on Socio Technological Shaping of Mobile Multi Media Personal Communications, 2002*. See at www.surrey.ac.uk/research.

Hildebrandt M; Gutwirth S., De Hert P. (eds.), '7.4: Implications of profiling practices on democracy and rule of law', FIDIS Deliverable WP 7D7.4, 2005, p 85.

Hildebrandt M; Backhouse J.(eds.), '7.2: Descriptive analysis and inventory of profiling practices', FIDIS Deliverable WP 7 ,2005, 116.

Hansen *et al*., *Privacy Enhanced Identity Management*, Information Security Technical Report, Vol. 9, number 1, Elsevier, Advanced Technology Oxford, 2004, pp.35–44.

Holznagel, B., Sonntag, M., 'A Case Study: The JANUS Project' in Nicoll, C., *et al* (eds.), *Digital Anonymity and the Law – Tensions and Dimensions*, TMC Asser Press, The Hague, 2003.

Hubaux, J. P., Buttyán, L., Capkun, S., *The Quest for Security in Mobile Ad Hoc Networks*, in: *Proc. 2nd ACM Symposium on Mobile Ad Hoc Networking and Computing - MobiHoc'01*, Long Beach, CA, USA, Oct. 2001.

IETF, *Ad Hoc Network Autoconfiguration Working Group. Ad Hoc Network Autoconfiguration (autoconf)*, 2006. See http://www3.ietf.org/html.charters/autoconf-charter.html.

Jenkins, *Categorization identity, social process and epistemology*, Current Sociology vol. 48, number 3, July 2000, pp.7 - 25.

Jiang, S., Vaidya, N. H., Zhao, W., *A Mix Route Algorithm for Mix-net in Wireless Mobile Ad Hoc Networks*, in: *Proceedings of the 1st IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS2004)*, pp.24–27 Oct 2004.

Josang *et al*., *Trust requirements in identity management*, Montague and Safavi – Naini (Eds.) Australasian Information Security Workshop 2005. Conferences in Research and Practice in Information Technology, vol. 44, 2005, p 99 – 108.

Karlg F., Schlott, S., Weber M., *Integrierte Sicherheit für Mobile Ad-hoc Netzwerke*, in: *Proc. 2nd German Workshop on Mobile Ad-Hoc Networks - WMAN 2004*, Ulm, Germany, Sep. 2004.

Kong, J., Hong, X., *ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks*, in: *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'03)*, pp.291–302.

Kuhn, T., *The Structure of Scientific Revolutions*, University of Chicago Press London, 1962, p 222.

Kuner, C., *European Data Privacy Law and Online Business*, Oxford University Press, 2003.

Lasen, A., *The social Shaping of fixed and mobile networks: a historical comparison 1*, Surrey Vodafone Scholar. Digital World Research Centre, University of Surrey, 2002, p. 44.

Luo, H. *et al*., *Self-securing ad hoc wireless networks*, in: Proc. 7th IEEE Symposium on Computers and Communications - ISCC 2002, Taormina, Italy, Jul. 2002, pp.567-574.

Lyon, D., *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University Press, 2001, p. 192.

Martucci, L. A. *et al*., *A Trust-Based Security Architecture for Small and Medium-Sized Mobile Ad Hoc Networks*, in: *Proc. 3rd Annual Mediterranean Ad Hoc Networking Workshop - Med-Hoc-Net*, Bodrum, Turkey, Jun. 2004, pp.278-290.

McDonalds, www.mcdonalds.com/corp/about.html; visited 2006-05-06, 2006.

Moukas, Al., *et al*., *Agent mediated Electronic Commerce II: Towards Next-Generation Agent-Based Electronic Commerce Systems*, Springer, 2000.

Rannenberg, K., *Identity management in mobile cellular networks and related applications*, in: Information Security Technical Report, Vol. 9, No. 1, 2004, pp.77-85, ISSN 1363-4127.

Reiter, M., Rubin, A., *Crowds: Anonymity for Web Transactions*, in: DIMACS Technical report, pp.97–115, 1997.

Ricoeur, P., *Oneself as another*, Chicago: Chicago University Press 1992.

Rodriguez Casal, C., Burgelman, J.C., Carart, G., *The Future of Mobile Communications in the EU: Assessing the potential of 4G*. Sevilla European Communities, Technical report series 21192 EN, 2004, p. 20. Available at ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf.

Roussos, P.D., Peterson, D., Patel, U., *Identity Management; an Enacted View*, International Journal of E - Commerce, vol. 8, number 1, M.E. Sharpe Armonk NY, 2003, pp.81–100.

Saärenpaä A., *The constitutional state and digital identity*, Paper available on the website of the 2002 World Congress for Informatics and Law II Spain September 23rd–27th http://www.ieid.org/congreso/ponencia_i.htm

Schiller, J., Voisard, A., Location-Based Services, Elsevier, San Francisco, 2004.

Seys, S., Preneel, B., *ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks*, in *International Workshop on Pervasive Computing and Ad Hoc Communications (PCAC06), Proceedings of the 20th IEEE International Conference on Advanced Information Networking and Applications (AINA 2006)*. IEEE Computer Society Press, 18th-19th Apr 2006.

Sorokin P;, *Social and Cultural Mobility*. New York: The Free Press, 1959.

Stajano, F. and Anderson, R., *The resurrecting duckling: security issues for ad hoc wireless networks*, in: *Proc. 3rd AT&T Software Symposium*, Middletown, NJ, USA, Oct. 1999.

Urry, J., *Mobile Sociology*, British Journal of Sociology, Blackwell Synergy, LSE, vol. 51, 2000, number 1, pp.185-203.

Vincke, J., *Sociologie. Een Klassieke Theoretische Inleiding*, UGent Press Gent,1998.

Walden, I., *Data Protection*, in: Reed C., Angel J., *Computer Law*, 5th edition, Oxford University Press, 2003.

Zhang, Y., Liu, W., Lou, W., *Anonymous Communication in Mobile Ad Hoc Networks*, in *Proceedings of the 24th Annual Joint Conference of the IEEE Communication Society (INFOCOM 2005)*, Miami, FL, USA, 13th–17th Mar 2005.

Zhou, L., Haas, Z. J., *Securing Ad Hoc Networks*, IEEE Network, vol. 13, i.6, pp.24-30, Nov./ Dec. 1999.

Zugenmaier, A., *FLASCHE – A Mechanism Providing Anonymity for Mobile Users*, in: Martin, D., Serjantov, D. (Eds.): *Privacy Enhancing Technologies*, 4th International Workshop, PET 2004, Springer-Verlag Berlin Heidelberg, 2005