FIDIS

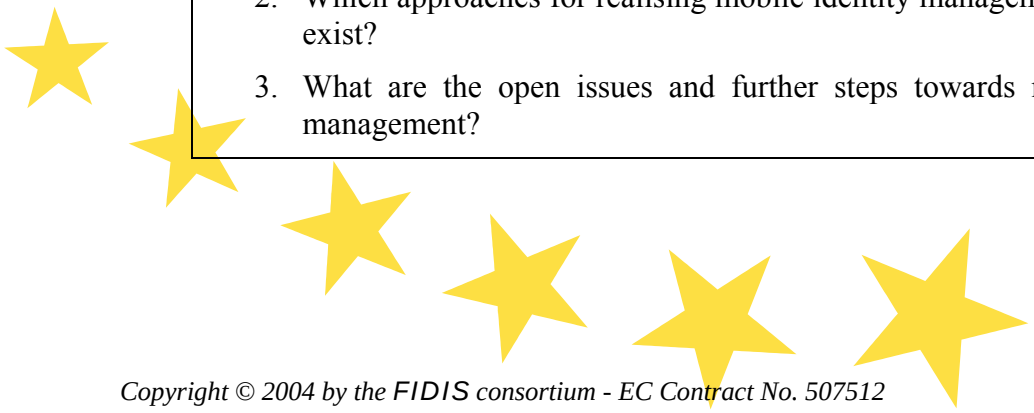
Future of Identity in the Information Society

Title:	"Study on Mobile Identity Management"
Author:	WP3
Editors:	Günter Müller, Sven Wohlgemuth (Albert-Ludwigs-Universität Freiburg, Germany)
Reviewers:	Jozef Vyskoc (VaF Bratislava, Slovakia)
	Mark Gasson (University of Reading, UK)
Identifier:	D 3.3
Type:	[Deliverable]
Version:	1.1
Date:	Friday, 10 June 2005
Status:	[Review]
Class:	[Work in Progress]
File:	fidis_wp3_del3.3_study_on_mobile_identity_management_v1.1.doc

Summary

Objective: This study gives a technical survey on mobile identity management. It identifies requirements for mobile identity management systems in particular on security and privacy of mobile users with mobile devices, e.g. smart phones or smart cards. A non-technical reader should understand the need and requirements for mobile identity management systems. Approaches for realising these requirements are described. The study gives answers to the following questions:

1. What are the requirements for mobile identity management systems in particular on user's mobility and privacy?
2. Which approaches for realising mobile identity management systems do exist?
3. What are the open issues and further steps towards mobile identity management?



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

Copyright Notice:

Members of the FIDIS consortium

Goethe University Frankfurt	Germany
Joint Research Centre (JRC)	Spain
Vrije Universiteit Brussel	Belgium
Unabhängiges Landeszentrum für Datenschutz	Germany
Institut Europeen D'Administration Des Affaires (INSEAD)	France
University of Reading	United Kingdom
Tilburg University	Netherlands
Katholieke Universiteit Leuven	Belgium
Karlstads University	Sweden
Technische Universität Berlin	Germany
Technische Universität Dresden	Germany
Albert-Ludwigs-Universität Freiburg	Germany
Masarykova universita v Brne	Czech Republic
VaF Bratislava	Slovakia
London School of Economics and Political Science	United Kingdom
International Business Machines Corporation (IBM)	Switzerland
Budapest University of Technology and Economics (ISTRI)	Hungary
Institut de recherche criminelle de la Gendarmerie Nationale	France
Netherlands Forensic Institute	Netherlands
Virtual Identity and Privacy Research Center	Switzerland
Europäisches Microsoft Innovations Center GmbH	Germany
Institute of Communication and Computer Systems (ICCS)	Greece
AXSionics AG	Switzerland
SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	21.12.2004	Initial release (Sven Wohlgemuth)
0.2	07.01.2005	Introduction of this study added (Sven Wohlgemuth)
0.3	17.01.2005	Scenario of ICPP extended by requirements for mobile identity management systems and new version of categorised survey on traditional and privacy-enhancing identity management mechanisms (Henry Krasemann, Martin Meints, Christian Krause)
0.4	17.01.2005	Contribution "Mobile Identity and Web Services" (Version 1) added (Joris Claessens, Christian Geuer-Pollmann)
0.5	18.01.2005	Structure redefined, introduction for the study revised, initial introductions for each chapter, description of identity manager *iManager* added (Sven Wohlgemuth)
0.6	22.01.2005	Addition of section 2.8 and some general minor corrections (Mark Gasson)
0.7	25.01.2005	Section "Categorised survey on identity management mechanisms ..." moved after section "Mobile Identity Management"; sections revised (Sven Wohlgemuth)
0.8	31.01.2005	Added outlook to WP11 (Denis Royer), syntax and usage corrected (Mark Gasson); sections revised, technical outlook added, review version (Sven Wohlgemuth)
0.9	10.02.2005	Review comments added (Mark Gasson)
1.0	28.02.2005	Contributions revised (all authors), Deliverable version (Sven Wohlgemuth)
1.1	10.06.2005	Spelling mistakes corrected (Sven Wohlgemuth)

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	Sven Wohlgemuth
2	André Adelsbach, Ammar Alkassar, Roger Cattin, Joris Claessens, Stefan Figge, Mark Gasson, Christian Geuer-Pollmann, Marit Hansen, Marcel Jacomet, Henry Krasemann, Christian Krause, Martin Meints, Lorenz Müller, Alain Rollier, Denis Royer, Sven Wohlgemuth
3	Christer Andersson, Simone Fischer-Hübner, Leonardo Martucci, Sven Wohlgemuth
4	Simone Fischer-Hübner, Jenny Nilsson, John Sören Pettersson, Sven Wohlgemuth
5	André Adelsbach, Ammar Alkassar, Christer Andersson, Roger Cattin, Simone Fischer-Hübner, Marcel Jacomet, Leonardo Martucci, Lorenz Müller, Alain Rollier, Sven Wohlgemuth
6	Denis Royer, Sven Wohlgemuth
7	Ammar Alkassar, Joris Claessens, Leonardo Martucci, Martin Meints, Lorenz Müller, Jenny Nilsson, Denis Royer, Sven Wohlgemuth

Table of Contents

1 Introduction

1.1 Scope

Every person has his own identity. This identity consists of person's roles, e.g. while using government services a person is well known whereas while he is shopping, only some personal attributes of him are needed. These different kinds of identity are represented by partial identities. A partial identity is a set of personal attributes of a user whereas a user can have several partial identities. Close to the physical world, a user changes his partial identity in computer networks while thereby varying between being anonymous and identifiable. Such a change depends on the situation. By this means, a user protects his privacy and at the same time is able to build up a reputation towards his communication partner with respect to his current partial identity.

A mobile user has several mobile devices such as mobile phones, smart cards or RFID (Radio Frequency ID). As mobile devices have fixed identifiers, they are essentially providing a mobile identity. Mobile identity takes into account location data of mobile users in addition to their personal data. Mobile identity management empowers mobile users to manage their mobile identities to enforce their security and privacy interests. Mobile identity management is a special kind of identity management. For this purpose, mobile users must be able to control the disclosure of their mobile identity dependent on the respective service provider and also their location via mobile identity management systems. This study focuses on this kind of mobile identity management: user-controlled mobile identity management.

The objective of this study is to give the non-technical as well as the technical reader a comprehensible, technical survey on mobile identity management, focusing in particular on security and privacy interests of mobile users. The study examines the need for mobile identity management by analysing scenarios and referring to literature. Requirements for mobile identity management systems are derived from exemplary scenarios. Privacy threats for mobile users and the usability of mobile identity management systems are both taken into account. Approaches for mobile identity management systems present the realisation of some requirements. A complete survey on the technical implementations of mechanisms meeting the described requirements and existing identity management systems (including mobile identity management systems) will be given in the FIDIS study on a "structured overview on prototypes and concepts of identity management systems" (D 3.1) and the "database on ID laws and identity management systems in the EU" (D 8.3). This study will end by drawing conclusions with an outlook to further research on mobile identity management.

1.2 Structure and Content

This study is divided into three parts:

- **Part 1: The need for mobile identity management**
- **Part 2: Exemplary security systems for mobile identity management**
- **Part 3: Conclusion and outlook**

The objective of the **first part**, which consists of chapters two, three and four, is to illustrate the need for mobile identity management by identifying the requirements for mobile identity management systems. These requirements are derived from interests of mobile users and service providers, focusing in particular on security for all participants and privacy for mobile

users. Exemplary scenarios describe the need of mobile user's identity and requirements for mobile identity management systems. Various mobile devices, such as mobile phones, smart cards and RFIDs as well as service architectures, such as Web Services, are considered. Ten mechanisms meeting the requirements for identity management systems are introduced and commented on with respect to mobile identity and mobile identity management systems. The first scenario on the use of a mobile identity management system using different profiles in different contexts shows the relevancy of those mechanisms especially related to mobility. In the context of mobile phones, the use of mobile identity for authorisation in GSM networks is illustrated together with a revenue model in which mobile users negotiate with service providers the sponsorship of their data transmission costs versus the disclosure of some attributes of their identity. The following scenario illustrates the conjunction of mobile user's identity in a GSM / UMTS network for authentication and billing purposes with Web Services. Potential privacy issues and possible solutions are outlined. As part of a mobile identity, the usage of RFID tags to bridge the gap between the physical and digital world and the link with the identity of a mobile user with its consequences for his privacy are outlined in the next contribution. The risk of identity theft by an intruder between this link, is topic of the next two contributions. Various mechanisms for linking a digital identity with a person authentication purposes such as single sign-on are discussed. Requirements for mobile identity management systems are derived.

Chapter three considers privacy threats for mobile users in detail. An attacker model for mobile users identifies the possibilities for an attacker to trace and identify a mobile user. Privacy threats for mobile users in *ad hoc* networks are described by scenarios and by using services for personalising the user interface of a mobile device in WAP based systems

Usability of an identity management system is important for its acceptance by its users, since security is not a user's primary objective. Therefore, chapter four describes the relationship between usability and security and presents user interface mock-ups for identity management systems.

The **second part** of this study aims at approaches for realising these requirements for mobile identity management systems. Chapter five considers anonymity systems as a basis for mobile identity management systems. Two anonymity mechanisms for mobile users are presented: location addressing and *mCrowds*. Location addressing empowers a mobile user to be anonymous, if his device does not have enough resources for using cryptographic algorithms or if no anonymity infrastructure is available. *mCrowds* establish an anonymity infrastructure without central servers for mobile users in order to minimise the dissemination of personal information on the mobile Internet. A comparison of anonymity mechanisms for *ad hoc* networks examines if current proposals and mechanisms for peer-to-peer anonymous communication protocols are suitable for *ad hoc* networks. Since a lot of anonymity services need an infrastructure, an approach for an anonymous incentive mechanism in order to establish an infrastructure in an *ad hoc* network is proposed.

A user is able to protect his identity by using partial identities towards his communication partners. As an example for a mobile identity manager, the research prototype *iManager* is described. An example illustrates the use of partial identities in order to protect the user's privacy. In order to link a digital identity with a person, a smart card system called *AXS ID-Card* is later described.

The **third part**, in chapter six, concludes the outcome of this study and provides an outlook to further research on mobile identity management. A glossary explains the fundamental terms

and acronyms which are used in this study. The principal concepts and terms of identity management are explained in the "inventory of topics and clusters" (D 2.1).

2 The Need for Mobile Identity Management

Exemplary scenarios illustrate the need of mobile user's identity and requirements for mobile identity management systems. Various mobile devices, such as mobile phones, smart cards and RFIDs as well as service architectures, such as Web Services, are considered. Ten mechanisms meeting the requirements for identity management systems are introduced and commented on with respect to mobile identity and mobile identity management systems. The first scenario on the use of a mobile identity management system using different profiles in different contexts shows the relevancy of those mechanisms especially related to mobility. In the context of mobile phones, the use of mobile identity for authorisation in GSM networks is illustrated together with a revenue model in which mobile users negotiate with service providers the sponsorship of their data transmission costs versus the disclosure of some attributes of their identity. The following scenario illustrates the conjunction of mobile user's identity in a GSM / UMTS network for authentication and billing purposes with Web Services. Potential privacy issues and possible solutions are outlined. As part of a mobile identity, the usage of RFID tags to bridge the gap between the physical and digital world and the link with the identity of a mobile user with its consequences for his privacy are outlined in the next contribution. The risk of identity theft by an intruder between this link, is topic of the next two contributions. Various mechanisms for linking a digital identity with a person authentication purposes such as single sign-on are discussed and requirements for mobile identity management systems are derived.

2.1 Categorised Survey on traditional and privacy-enhancing Identity Management Mechanisms which are relevant for Mobile Identity Management

The following categories and mechanisms are derived, among others, in Identity Management Systems (IMS): Identification and Comparison Study[1]. The categorisation is a commented listing of categories of special importance and special requirements for Mobile Identity Management Systems.

I. Functionality: Identity Administration
   a. Communication-independent handling and representation of identities: Possibility to choose between different profiles / data schemes; Creating, updating, deleting identity and identity information
   b. Pseudonyms with specific properties: Using pseudonyms for privacy enhancing by averting linkability
   c. Credentials: Credentials are convertible certifications for authorisations which a user has obtained by use of a pseudonym. These credentials can be transferred to his other pseudonyms without being transferred to other users' pseudonyms. Although an authorisation is bound to an individual and can be reliably used in many contexts, its use does not lead to data trails or unwanted disclosure of personal data. As long as the individual does not misuse the credential, anonymity is guaranteed.
      i. Becoming increasingly important, as mobile devices are acting as interfaces for ambient computing and are substituting different cards (e.g. credit cards, health cards etc.)
      ii. Examples: proof of majority / driving licence
   d. Identity recovery

II. Functionality: Notice
   a. History Management: Possibility to log transaction for reconstructing and analysing data flow
      i. Example: Illustrating what the communication partner knows from previous transactions
   b. Context detection: which partial identity was used in which transactional context

III. Functionality: Control
   a. Rule Handling
      i. Special mobile devices e.g. RFIDs are designed to have no rule handling for the person carrying the device and are therefore discussed as potentially privacy violating. Rule handling becomes especially important when mobility together with location based data is involved.
      ii. Support user to choose the right profile / preferences etc.
   b. Anonymity as base-rule for privacy enhancing
      i. Essential on the lower layers to enable Identity Management
      ii. Anonymity is also seen as mechanism for security, especially confidentiality

IV. Security (the following aspects of Security are taken from[1] the IT-Baseline Protection Manual[1] and the British Standards (ISO/EIC 17799)[2])
   a. Confidentiality (e.g. anonymity, secrecy)
      i. Techniques to enable anonymity have to be developed for the use of mobile devices and location based data used with location based services
   b. Integrity (including non repudiation)
   c. Availability

V. Privacy
   a. Privacy control functionality (consent, objection, disclosure, correction, deletion and addition of privacy information)
      i. Example: The privacy control functionality has to include location data → give user the possibility to control the flow of location data himself
   b. Data minimisation: Storing and processing only data which is really necessary
   c. Standards (e.g. P3P), seals (e.g. Datenschutz-Gütesiegel beim ULD SH) and penalties

VI. Interoperability and Gateways
   a. Compliance to existing standards
      i. Standards are special for mobile devices
   b. Interfaces

1 See: www.bsi.de

2 E.g., www.iso17799-web.com

i. Interfaces are special for Mobile Devices

VII. Trustworthiness
   a. Segregation of power, separating knowledge, integrating independent parties
   b. Using Open Source
   c. Trusted seals of approval

VIII. Law Enforcement / Liability
   a. Digital evidence
      i. Example: Proof of transactions etc.
   b. Digital signatures
   c. Data retention
      i. Comment: this is in contrary to privacy

IX. Usability
   a. Comfortable and informative user interfaces
      i. Interfaces for mobile devices have to be developed for the special need of different displays etc. (touch screen, speech, etc.)
   b. Training and education
   c. Reduction of system's complexity
   d. Raising awareness

X. Affordability
   a. Power of market: Create MIMS that are competitive and are able to reach a remarkable penetration of market
   b. Using open source building blocks
   c. Subsidies for development, use, operation, etc.

As outstanding mechanisms for the handling or the representation of identities, the different types of pseudonyms and credentials play a particular role. By use of these mechanisms, the core concept of the "user-controlled, technology-based Identity Management" can be realised technologically also for Mobile Identity Management.

2.2 Scenario of the use of Mobile Identity Management Systems

2.2.1 Introduction

In section 2.1, the main mechanisms for Mobile Identity Management Systems (MIMS) are introduced. The following simple scenario will show how essential the first six mechanisms are for the functionality and privacy-compliance of MIMS. The mechanisms and the subcategories used in this scenario are listed at the end of this chapter.

It is difficult to show the mechanisms related to market and user acceptance (mechanisms VII to X (trustworthiness, law enforcement and liability, usability and affordability)) in an intuitive scenario. They are not just specific to MIMS, but important for Identity Management Systems in general. These mechanisms are therefore discussed in the FIDIS study on a "structured overview on prototypes and concepts of identity management systems" (D 3.1).

Relevant aspects concerning usability of Identity Management Systems on mobile devices are discussed in chapter 5 of this document.

2.2.2 Starting Point

Alice has a mobile device, which is connected via GPRS / UMTS to a service provider for location based services. Examples for those location based services are local restaurant guides or the service "friend finder".

The mobile device is equipped with a Mobile Identity Manager System. This software allows Alice to edit, store and select various service specific personal profiles to be used for location based services. Those profiles are understood as Partial Mobile Identities.

In this example, profiles are locally edited, selected and stored; the user of the device is in control of those profiles and their use including history logging. In addition, the Mobile Identity Management System stores all transactions of data from profiles to location based service providers. This functionality can be used to illustrate the flown data and, e.g., to comprehend bills of the service provider with service-requests by the user.

Alice has pre-configured some profiles – e.g. a professional one with her preferences for business lunches and a private one for her personal preferences at weekends and holidays. The professional profile contains, in addition, data about her business contacts, the personal one about her friends.

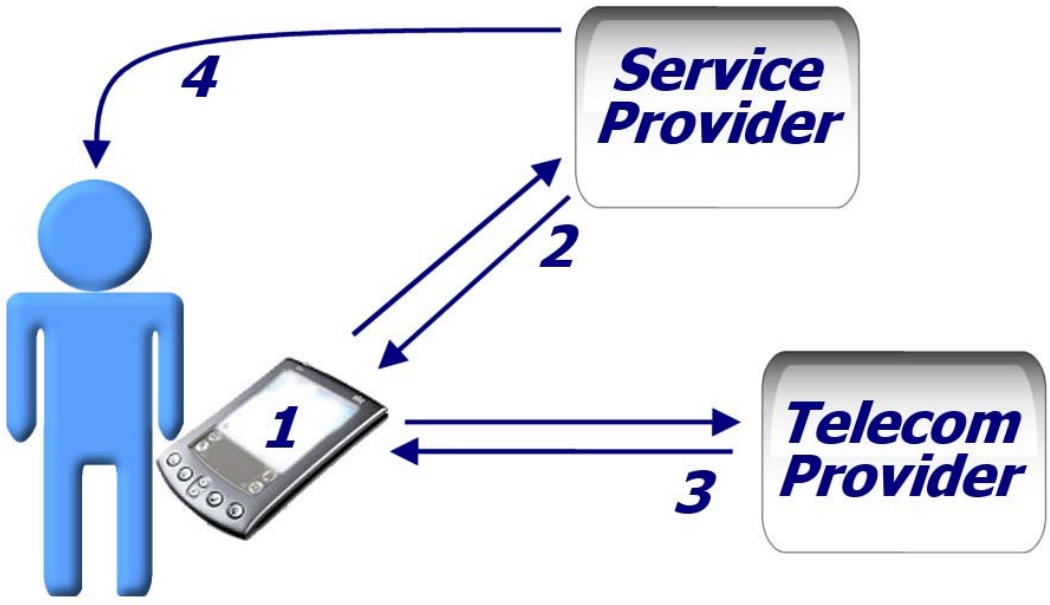


Figure 1-1: Overview of the communication process of the restaurant finding service

2.2.3 Scenario 1: Finding a local restaurant for a business lunch

Step 1

Alice selects her professional profile after starting her mobile device.

Step 2

She selects the service "local restaurant finder" to find a nearby restaurant for a business lunch. The service provider gets the pre-selected preferences of Alice concerning the quality (in this case high) and preferred Asian (she likes Asian food and most of her business contacts do as well). The service provider has to know where Alice is located so and asks for the location data.

Step 3

Depending on the technical specification of her mobile device (e.g. GPS-locator integrated) or her preferences (e.g. manual input of her current location) the mobile device gets the location automatically from the GPS locator or the telecommunication provider or Alice has to enter it manually. The MIMS submits this information after acknowledgement to the service provider.

Step 4

The service provider sends a list of restaurants in the requested specification to Alice's mobile device together with geographic information (e.g. maps) showing how to reach them from her current position.

2.2.4 Scenario 2: Finding a local restaurant for a private lunch

Step 1

Alice selects her private profile after starting her mobile device.

Step 2

She selects the service "local restaurant finder" to find a nearby restaurant for her private lunch. The service provider gets the pre-selected preferences of Alice concerning the costs and the quality (in this case she prefers fast-food due to her lack of time). The service provider has to know where Alice is located so asks for the current location data.

Step 3

The mobile device gets the location automatically from the telecommunication provider. The service provider has to know where Alice is located and asks for the location data.

Step 4

The service provider sends a list of fast-food restaurants to Alice's mobile device together with geographic information (e.g. maps) showing how to reach them from her current position.

2.2.5 Required mechanisms for Mobile Identity Management Systems

To enable the two scenarios, the Mobile Identity Management has to support the following mechanisms listed in section 2.1:

1. Function Identity-Administration
   - Communication-independent handling and representation of identities: Possibility to choose between different profiles
2. Function Notice
   - History-Log over the use of the profiles and the flown data in the MIMS
3. Function Control
   - Rule-Handling performed by pre-editing the profile and transferring the location data to the service provider
4. Privacy
   - Privacy-control and data minimisation can also be handled in the pre-edited profile; the service-provider doesn't necessarily need to know, who is using the service as long as it is paid; this could e.g. be carried out using pseudonyms being certified by a trusted third party (e.g. a bank).
5. Security
   - Confidentiality and integrity of the profiles and the MIMS; availability of the MIMS
6. Interoperability and Gateway
   - E.g. necessary to transfer the location data from the telecommunication provider to the service provider

2.3 GSM-based Mobile Identity Management

GSM's success is very much due to comprehensive identity management based on the Subscriber Identity Module (SIM). The SIM concept, together with the supporting GSM infrastructure, provides both identity and security for accessing mobile voice and data services. With existing GSM roaming functionality, the SIM card is one of the most distributed and technologically adopted identification concepts worldwide, enabling mobile phone users to access telecommunication services in many regions all over the world:

- Subscriber Identity Module (SIM) provides an infrastructure with a reliable technical foundation (e.g. Public Key Infrastructure (PKI))
- A mobile identity in this definition is inherently related to the mobile network operator business
- Represents contract between subscriber & network operator
- Authorises subscribers to use the network
- Allows subscribers to authenticate themselves
- Over 1 billion GSM subscriptions (IDs) (http://www.gsmworld.com)

- More countries with SIM infrastructure (197, May 2003) than with McDonald's restaurants (119, Aug 2003) and more than UN member states (191, Aug 2003)

In emerging UMTS networks, the Universal Subscriber Identity Module (USIM) will take over the SIM's functionality and will provide enhanced security features, such as mutual authentication, in 3G networks. In this context, the following issues are part of mobility and identity research:

2.3.1 Elements of a mobile identity

Mobile communication networks provide a number of services. Among them, new data services in the shape of M-Commerce applications or mobile information services are important future applications. With current mobile identification concepts, the main focus is to provide simple, easy-to-handle identities in order to technically enable secure communication and to cover billing issues. For the named data services, advanced identity concepts are needed. Unlike the static identity already implemented in current mobile networks, dynamic aspects like the user's position or the temporal context increasingly gain importance for new kinds of mobile applications. Some of the arising questions to be answered in that context are:

- What information is necessary to describe a mobile user's identity and to represent the current mobile situation and context (e.g. location, personal and general preferences and temporal constraints)
- What technical standards can be applied in order to obtain access to these different components of a mobile identity (mark-up languages, architectures, etc)
- Which parties in addition to the mobile user have to be involved to form a mobile identity and how can they exchange information (e.g. mobile network operators, service or profile providers)
- Will it be necessary to introduce group identities pooling single subscribers, e.g. to simplify administrative tasks

2.3.2 Profile management

As a result, an advanced mobile identity is a more complex object than current SIM-centric identities. Personal information about users, collected in profiles, is used to determine the mobile identity of users. An exemplary user profile could store a user's home and workplace locations, his daily schedule (regular trips from and to work) and so on. All this information has to be manageable by the user and must be assembled in a standardised format, such that different service providers are able to understand and utilise the information. The User Agent Profile Drafting Committee of WAP Forum/Open Mobile Alliance created a specification of a framework for conveying user agent profiles containing information on preferences and capabilities associated with users and user agents when accessing resources on Mobile Internet (WAP) sites. User agent profiles enable personalisation of sites, which is an important prerequisite for providing usability for mobile Internet devices with small displays.

As for the management of that kind of information, there are only a few established editing concepts (they are seldom limited to text). Appropriate new ways to manage that kind of information have to be identified. Another arising question is, where and how these different time or location specific profiles will be stored. Some information may reside at the network operator side while others may be stored directly on the mobile terminal. The information

may be encrypted before it is stored on the device or transmitted to the network operator. The question of profile allocation and aggregation has to be discussed. New strategies for profile management also have to include adequate privacy concepts, such as the use of Privacy Enhancing Technologies (PETs).

2.3.3 Exchanging mobile identities

The current mobile identification infrastructure is used mainly by mobile network operators. As these follow more or less equivalent rules and security regulations, security concerns have only seldom been raised. For new mobile services, the identity of a mobile user is intended to be accessible by any third party that offers mobile services. In that context, new approaches to secure the mobile identity and to exchange identity information have to be outlined and discussed. The current legal landscape already limits the way of how to reveal mobile identity information. Legally compliant ways to exchange that information have to be identified and outlined. One way to address these challenges is the introduction of policies for the negotiation of exchanged information.

2.3.4 Applications for mobile identities

The main application for a publicly accessible, comprehensive mobile identity is the individualisation and sponsoring of mobile business relations. If mobile network operators in cooperation with the service user are able to supply service providers with a mobile user identity including the user's geographical, temporal and personal context and preferences, the service provider is able to extensively individualise the provided service and to provide context-aware services. The service provider could also decide to sponsor the data communications costs the user would normally have to pay. In that way, new business models can be applied in order to realise a reverse charging where service providers are paying mobile network operators in order to gain a communication channel to potential customers and to transfer marketing messages. This new business model may find its way from the mobile to the fixed Internet environment and thus have an impact on location based service related identities for this medium. Additionally, mobile government applications such as disaster management (e.g. warning people of flooding or locating them via their mobile for rescue) are based on mobile identities.

2.4 Revenue Models for M-Commerce with Mobile Identity

Current mobile business models for mobile commerce do not seem promising with regard to substantial revenue streams for mobile network operators as well as mobile service providers. Today's settings require customers to "invest" in data transmission (GRPS as well as UMTS and WLAN data) before being able to use a mobile service, i.e. they are forced to pay for all data transmitted regardless of whether this data is of valuable content or just unwanted marketing messages.

2.4.1 Architecture

An approach for a new business model is to allow mobile service providers to apply information about the mobile identity of the customer as situation based profiling. It enables service providers to identify high value customers and to sponsor their data transmission costs. It can be shown, that by applying this approach revenue streams can be increased significantly for all parties involved, contributing to a more positive perspective for future developments in the mobile market.

In order to apply a more complex form of interaction, the service provider has to be offered more and richer information about its customers. Only with a comprehensive, reliable and up-to-date-description of the customer the service provider is able to differentiate between relevant and non relevant customers and to determine, how much he is willing to invest into any customer. To put it in other words: The service provider has to have a clear idea of the customer's business value in the current situation. The information describing the customer's situation is generated by the mobile network operator and then transmitted to the service provider (Figge, 2001). The process in detail appears as follows:

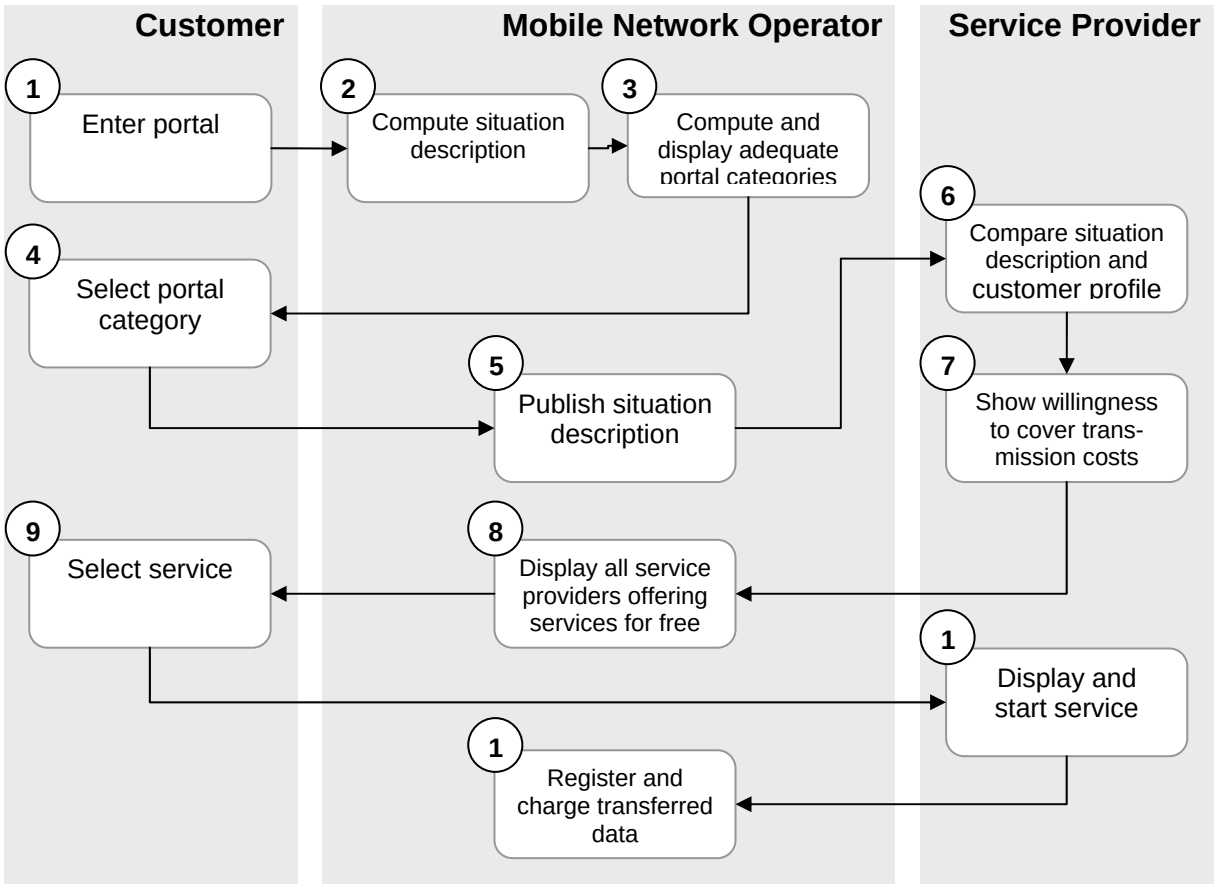


Figure 2-2: Portal process for a situation based business model (Figge, 2003)

By entering the mobile portal (1), which is provided by the mobile network operator, the situation of the mobile customer is captured and portal categories relevant for that situation are displayed (2+3). E.g. if the current local time is near noon and if the customer is not familiar with his current location, the category "Restaurants & food" might be of interest. Whereas in the afternoon right within a business meeting that category does not seem to be appropriate. The customer selects one category (4) and his situation description is transferred to all service providers with services assigned to that category (5). Using the situation description, service providers can decide if the customer seems to be relevant for their business (6) in which case they cover the data transmission costs (7). After selecting the portal category, all service providers willing to do that get listed (8). The customer chooses one of

the services (9) and the transmission costs are being billed to the respective service provider (10+11).

The decision of a service provider, whether a customer is business relevant or not, typically follows an automated process. Ideally, a target customer profile is being compared to the current dynamic profile available. The issue of profile matching is not being discussed here in detail, but typically several criteria are the basis for customer selection. The following example is used to illustrate this process.

A chain of department stores in Frankfurt and Berlin with regular opening hours offers its customers a mobile shopping assistant service. A target customer profile has been created to catch middle-aged customers within the reach of the branches. With the opening of the portal category 'Shopping' the situation description of the requesting customer is transferred to the company and then compared to the target customer profile. Figure 2-3 illustrates three sample cases to show potential results of the process:

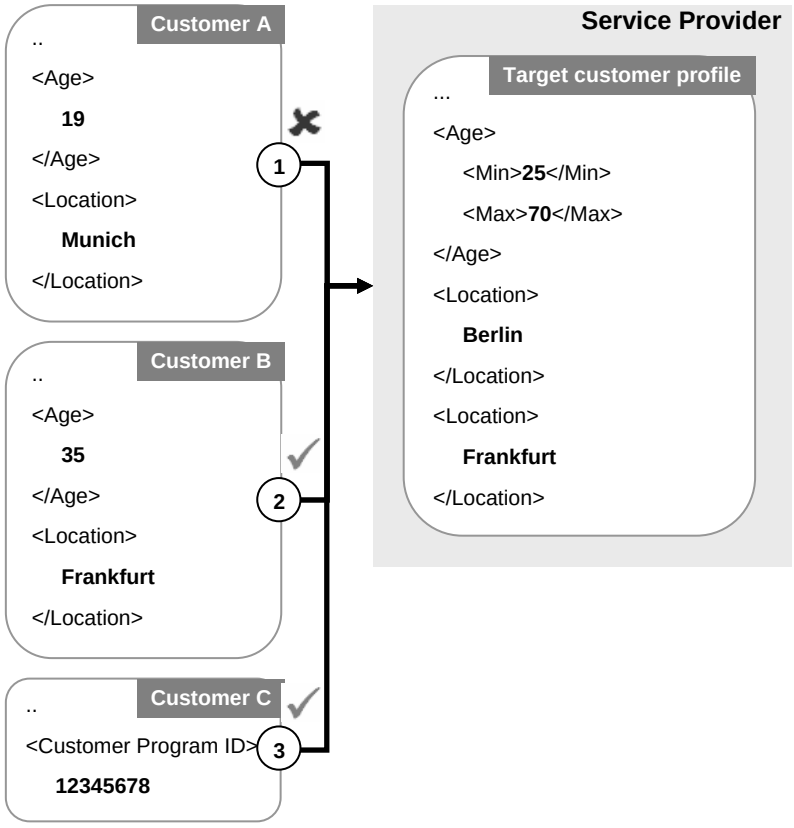


Figure 2-3: Matching situation description and target customer profile (Figge, 2003)

Customer A's situation description and its properties (1) do not match the properties of the service provider's target customer profile. Neither age nor current location fit to the target properties. Sponsoring customer A does therefore not seem to be appropriate. In this case the service provider will deny paying the charges (of course, this does not prohibit the customer from still choosing the service). The situation is different for customer B (2), whose relevant properties are matching. In this case the investment is promising, as the chances of the customer visiting the department store and generating revenue are high. The situation is even

more obvious for customer C (3) who participates in the company's customer loyalty program and is therefore registered. In case the service provider holds information about the customer's past purchasing patterns it is easy to decide if an investment in terms of offering a free mobile channel makes sense from an economic point of view

2.4.2 Summary

With this new approach, current revenue models are enhanced by including the service provider. The mobile customer still remains an important source of revenue in terms of mobile voice telephony and mobile services targeting direct revenues, but the existence of a chargeable service provider reduces the pressure to search for revenue at the customer's side only. By including the service provider, the usage of the mobile Internet gets more attractive as the choice of available services increases and becomes more cost efficient at the same time.

The pricing models offered to service providers can differ from those used for private customers. Instead of millions of mobile customers only a few hundred or thousand of service providers are interacting with the mobile network operator. That enables the implementation of flexible and individual tariff models, cross trading, lump sum payment etc. and opens up a new flexibility for marketing strategies.

The new business model therefore provides an adequate distribution of the revenue streams and allows the mobile customer to save money, too.

2.5 Mobile Identity and Web Services

The Internet has become a very common and natural way for business interactions and information exchange between organisations and among individuals. Nearly everyone is familiar with email and the World Wide Web. Web Services are the next step in this interconnected world. They bring the paradigm of service-oriented architecture in practice. They offer an interoperable framework for stateless, message-based and loosely-coupled interaction between software components. These components can be spread across different companies and organisations, can be implemented on different platforms and can reside in different computing infrastructures. Web Services can expose any useful functionality on the Internet via XML messages that are exchanged through a standard protocol, called SOAP. These message exchanges can happen in a secure, reliable and transacted way, between federated organisations, or between peer individuals. See (Cabrera, Kurt and Box, 2004; IBM Corporation and Microsoft Corporation, 2003) for more information. The Web Services federated security architecture is also discussed in the FIDIS study on a "structured overview on prototypes and concepts of identity management systems" (D3.1).

In parallel to the Internet growth, mobile communications have become an additional common way of interconnecting. There has been a vast penetration of mobile phones and devices over the last years. Most people have a personal mobile phone or mobile device. As these devices (or more accurately, the SIM, WIM or USIM, see section 2.3) have fixed identifiers, they are essentially providing a mobile identity. Mobile network infrastructures provide the means for authentication and billing of this identity.

Bridging these two worlds would be advantageous. Mobile operators could then for example provide (web) services that give access to mobile services. Third party service providers could leverage the authentication and billing infrastructure of mobile networks, instead of setting up and maintaining their own identity management systems (e.g., usernames and passwords).

The Mobile Web Services initiative (Microsoft Corporation and Vodafone Group Services Ltd., 2003) forms a motivational background for this study. Note, however, that the content of this section does not necessarily reflect in any way the technical roadmap or outcomes of this specific initiative. The combination of WWW and wireless security has also been explored in (Claessens, Preneel and Vandewalle, 2002).

This chapter touches upon potential Mobile Web Services scenarios and specific associated privacy requirements. While the chapter points to some mechanisms and approaches with which these privacy goals can be addressed, complete architectures and solutions are out of the scope.

2.5.1 Mobile Web Services scenarios

Figure 2-4 below describes the possible Mobile Web Services scenarios, which are largely based on, but not necessarily duplicating, scenarios described in (Microsoft Corporation and Vodafone Group Services Ltd., 2003).

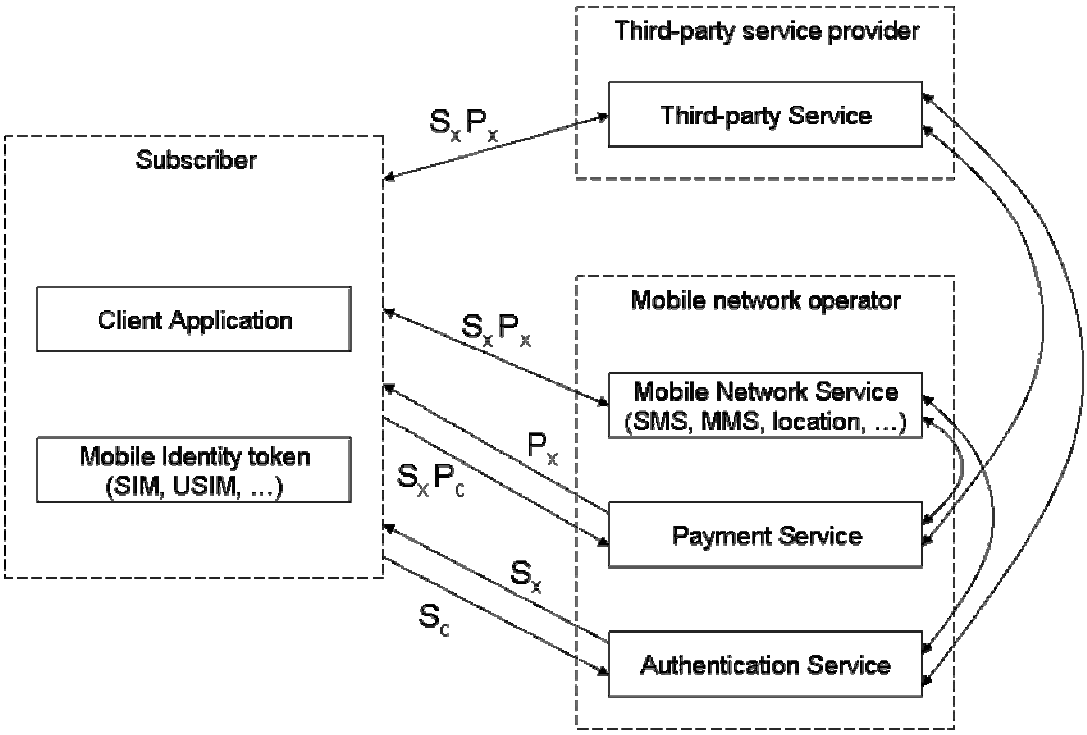


Figure 2-4: Mobile Web Services scenarios, based on (Microsoft Corporation and Vodafone Group Services Ltd., 2003)

There are three entities participating:

- The Subscriber is a user who has a mobile identity token from a mobile network operator, either a pre-paid card, or mobile subscription.
- The Third-party service provider provides Web Services exposing specific business or entertainment value. The Third-party service provider has a business relationship with the Mobile network operator to leverage the mobile network authentication and billing infrastructure when the Subscriber wants access to the third-party web service.

- The Mobile network operator provides specific authentication and payment web services, as well as specific mobile network Web Services, such as SMS, MMS and location provision. The specific mobile network Web Services require the Subscriber to authenticate and optionally pay.

For the purpose of this chapter, the Subscriber's Client Application and Mobile Identity token are able to connect and exchange information in some way and are abstracted as one component. Both third-party services and mobile network services may interact with the mobile network operator's authentication and billing infrastructure in the back-end (e.g., to settle payment).

When a Client Application wishes to make a secure service request to either a Third-party Service or a Mobile Network Service, it may be required to obtain a Security Token (S_x) from the Authentication Service. When the Authentication Service receives a request to issue a Security Token, it will typically require a certain Service Context (S_c) of the service request being made, where the Service Context may for example detail the Mobile Network Service or Third-party Service the Client Application wishes to access. The Authentication Service will then issue a Security Token if it can successfully authenticate the Subscriber by using the Mobile Identity token authentication mechanism.

If the service request to either the Third-Party Service or Mobile Network Service also involves payment, the Client Application must obtain a Payment Token (P_x) from the Payment Service, typically once it has obtained the appropriate Security Token. When the Payment Service receives a request to issue a Payment Token, it requires the Payment Context (P_c) of the service request being made, where the Payment Context may for example detail the payment amount required by the Third-Party Service or Mobile Network Service. The Payment Service will issue a Payment Token if it can successfully obtain payment authorisation from the Subscriber.

Note that the scenario in section 2.4 focuses on profiling of mobile customers by the mobile operator, for the purpose of offering *mobile* services where the data transmission cost may be covered by the service provider. We here discuss the use of the authentication and billing infrastructure of mobile networks for the purpose of authenticating to, and billing, *Web* services (offered by service providers as well as the mobile operator).

2.5.2 Privacy objectives related to billing/payment

In the billing or payment scenario the mobile operator effectively acts as the bank in a classical electronic payment system (Claessens, 2002), as indicated in figure 2-5.

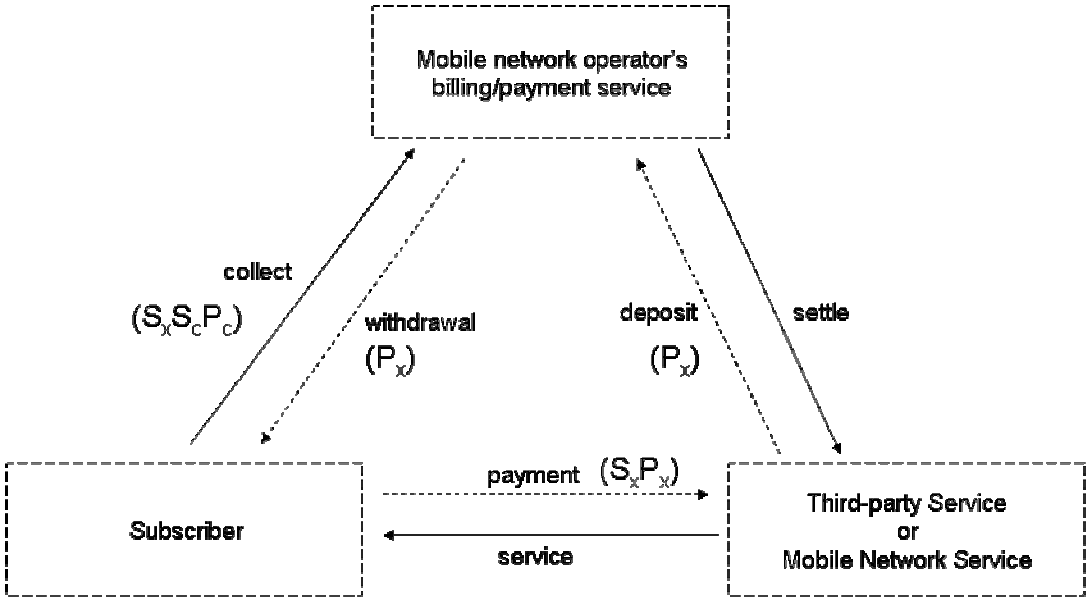


Figure 2-5: Classical electronic payment system applied to mobile network billing

The Subscriber's privacy requirements are generally related to the *unobservability*, *untraceability* and *unlinkability* of the Subscriber's identity with respect to external observers as well as with the participating entities. These requirements originate from the electronic payment systems world (Claessens, 2002) and are also aligned with the generic anonymity requirements defined by (Pfitzmann and Hansen, 2004).

- Unobservability – External parties should not be able to observe the Subscriber's identity from ongoing Web Services interactions. If the Subscriber's identity is not encoded in any of the security tokens or contexts, it cannot be observed. If it is encoded, then it should be confidentiality-protected by using the necessary Web Services security protections.
- Untraceability – For a single transaction, neither the mobile network operator nor the third-party service provider should be able to trace the identity of the Subscriber in the context of a 'payment' or a 'deposit' transaction. This means that the Subscriber's identity should not be disclosed from the Subscriber to the Service as part of using the payment token and from the Service to the Mobile Operator as part of depositing the token. This particularly also means that the mobile operator should 'blindly' issue a payment token, so that it cannot be linked to the Subscriber's identity when it is later deposited by the service provider.
- Unlinkability – The mobile operator or the service provider should not be able to link multiple transactions as originating from the same Subscriber.

There are other privacy issues besides the Subscriber's identity. In case where the Subscriber's identity is known by the mobile network operator and the service provider, then at least the specific service context (e.g., goods obtained through the service) should not be disclosed to the mobile network operator.

In addition to the privacy requirements, there are a number of security requirements which need to be addressed at the same time. Most importantly these include the detection and/or

prevention of double-spending. A complete overview of these security requirements is beyond the scope of this chapter.

The generic Mobile Web Services scenarios as well as the Web Services security specifications allow the usage of custom token profiles which can leverage different types of electronic payment system structures. Orthogonal to (but sometimes dependent of) the privacy requirements, these can have different characteristics:

- The Subscriber can have a *local* or *central* account. If the Subscriber can obtain payment tokens which actually carry monetary value, the Subscriber can maintain a local account on his device. The payments can also directly come from a central account associated with the Subscriber and maintained by the mobile operator. Both pre-paid phone card and mobile subscription can support local and central account.
- There can be *pre-payment* or *post-payment*. If the mobile network operator collects money from (or adds to the bill of) the subscriber at the time of withdrawing the payment token, we refer to pre-payment. If the subscriber gets a bill from the mobile network operator after the payment token has been deposited, we refer to post-payment. Both pre-paid phone card and mobile subscription support pre-payment. Post-payment is only possible with a mobile subscription.
- Electronic payments can be *on-line* or *off-line*. A payment is on-line if the service provider has to deposit the payment token immediately after payment and before providing the service, essentially to verify if the payment will be covered. If the deposit can happen at a later point in time without the service provider needing to worry, we refer to an off-line payment transaction.

2.5.3 Privacy objectives related to authentication

While payment can be generalised into authorisation, authentication really refers to identity authentication. The privacy goals are therefore somewhat different.

We particularly look more closely at the case of the third-party service provider, wanting to leverage the mobile network operator's authentication service (e.g., an e-commerce service provider that wants to authenticate its customers, or an organisation that wants to authenticate its employees).

We can identify the following potential privacy requirements:

- It may be required that the mobile network operator does not learn anything else but the mobile identity of the subscriber. The subscriber should be able to authenticate to the operator (using the mobile identity token) without specifying any service context and obtain a security token that only asserts the subscriber's mobile identity, which can be used for any third-party service. The mobile network operator and especially the third-party service provider should be sure that only the subscriber can prove ownership of the security token. The security token should only be valid for a limited amount of time to ensure freshness of the mobile authentication.
- It may be required that the third-party service provider is not able to learn the real mobile identity of the subscriber (i.e., mobile phone number), but a registered pseudonym instead. The mobile operator's authentication service may effectively act as a pseudonym service, issuing security tokens that assert a pseudonym. The operator is able to map the mobile identity to the appropriate pseudonym. (Authorised entities would also be able to

ask the operator to map a pseudonym to a mobile identity.) Such a pseudonym service may also be provided by a third-party service provider. In order to obtain a pseudonym a specific registration interaction between the final service, the pseudonym service and the subscriber would be needed.

2.5.4 Discussion / conclusion: Summary of requirements

This chapter analysed the generic privacy objectives related to billing/payment and authentication within mobile web services scenarios. Referring to the categorised survey on traditional and privacy-enhancing identity management mechanisms relevant to mobile identity management (see section 2.1), this chapter focused on the following specific privacy requirements:

- I.b. Pseudonyms (for authentication means)
- I.c. Credentials (in the form of payment authorisations)
- VI Interoperability and Gateways (Mobile Web Services standards)

Note that while this chapter focused on the specific privacy requirements above – concentrating on the interactions between the entities – most other privacy requirements that are listed in the survey, would be relevant to overall Mobile Web Services solutions as well.

2.6 Scenario – Ubiquitous Computing

So far, discussion has been limited to mobile technologies that are currently in circulation, in essence where issues of security and privacy within the identity context are already of paramount importance. In order to fully explore the importance of mobile identity management in this section we shall extrapolate existing technologies and consider a further scenario in which emerging technologies are prevalent.

2.6.1 Ambient Intelligence environments

The emergence of both the Internet and wireless network technology and with them the possibilities of distributed computing (i.e. using several computing devices that are not necessarily located in the same geographic location, for a specific task) has had a profound effect on our way of life. Building on these advancements, Ubiquitous Computing (Weiser, 1991) is the next wave of technology, a paradigm shift from our current relationship with technology, whereby many thousands of wireless computing devices are distributed in the environment in everyday objects around us.

Ubiquitous Communication will allow robust, *ad hoc* networks to be formed by this broad range of mobile and static devices, forming a ubiquitous system of large-scale distributed networks of interconnected computing devices. By adding intelligent user interfaces and integrating sensing devices, it is possible to identify and model user's activities, preferences and behaviours, forming individualised profiles. These key aspects are all required to achieve the idealised Ambient Intelligence (AmI) Environment (figure 2-6), a concept which has been formalised by the European ISTAG[3].

3 *Information Societies Technology Advisory Group*

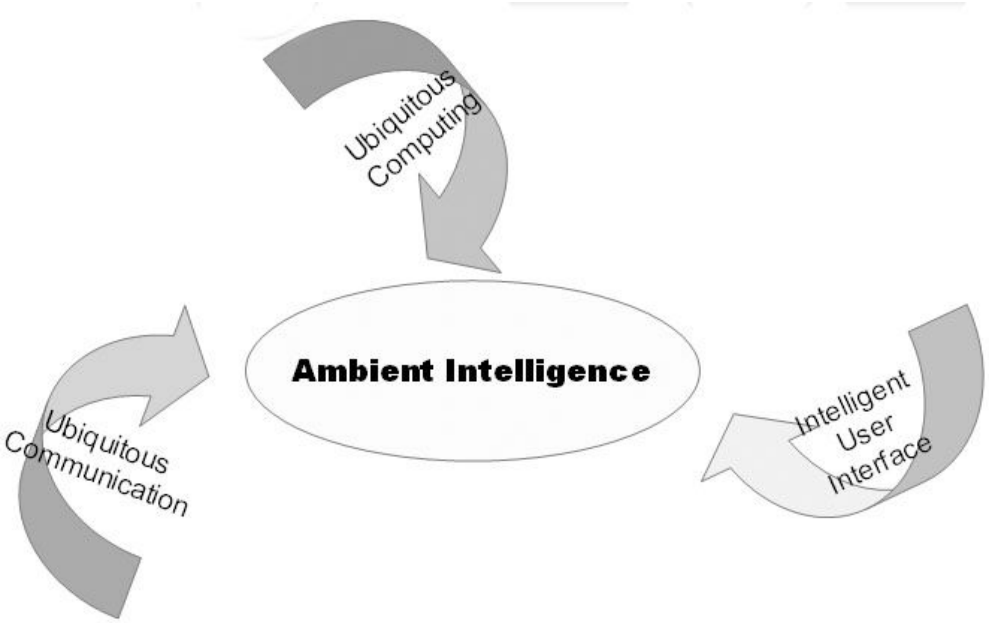


Figure 2-6: The key components of the AmI scenario

The aim of the AmI environment is to provide a context aware system, using unobtrusive computing devices, that will improve the quality of people's lives by acknowledging their needs, requirements and preferences and thus acting in some way on their behalf. To achieve this, the 'intelligent' environment needs to build up a profile of each individual and be able to subsequently link that profile with the correct individual. In essence, the environment has become the interface to the distributed and invisible AmI. In a world where computing is truly ubiquitous, the environment will monitor direct interaction of people with objects. Profiles will seamlessly follow the individual with whom they are linked.

The main concern from the technological viewpoint with this future scenario is the very real problem of power. There needs to be a method by which embedded computing devices are powered when required, but without the user ever needing to know that they are there. A proposed solution to this is the use of Radio Frequency IDentifiers (RFID) which are powered wirelessly and externally by the device which attempts to read it. The first clear step towards the Ubiquitous Computing scenario is the use of RFID tags in supermarket product packaging. RFID tags are *unique* identifiers which allow an individual item (not just type of product) to be wirelessly detected. In this way they are more useful to the supermarket than product barcodes, since the tags cannot only identify the product (and thus the price at the till), but which batch it actually came from and other data regarding its history that may have been logged. Ultimately, the aim is to tag every item sold, including food, clothes, electronic goods and medicine (FDA, 2004); with an Internet database that holds a record of every item. Current trial applications have gone one step further with the tagging of people for tracking purposes. In 1998, research at the University of Reading, UK enabled the Cybernetics building to track and build personal profiles of people with surgically implanted RFID tags, one of the earliest AmI environment applications.

2.6.2 Required mechanisms for Mobile Identity Management Systems

Given this potential scenario, in this context, it is useful to access the potential requirements of mobile identity management systems. Consider the scene in figure 2-7:

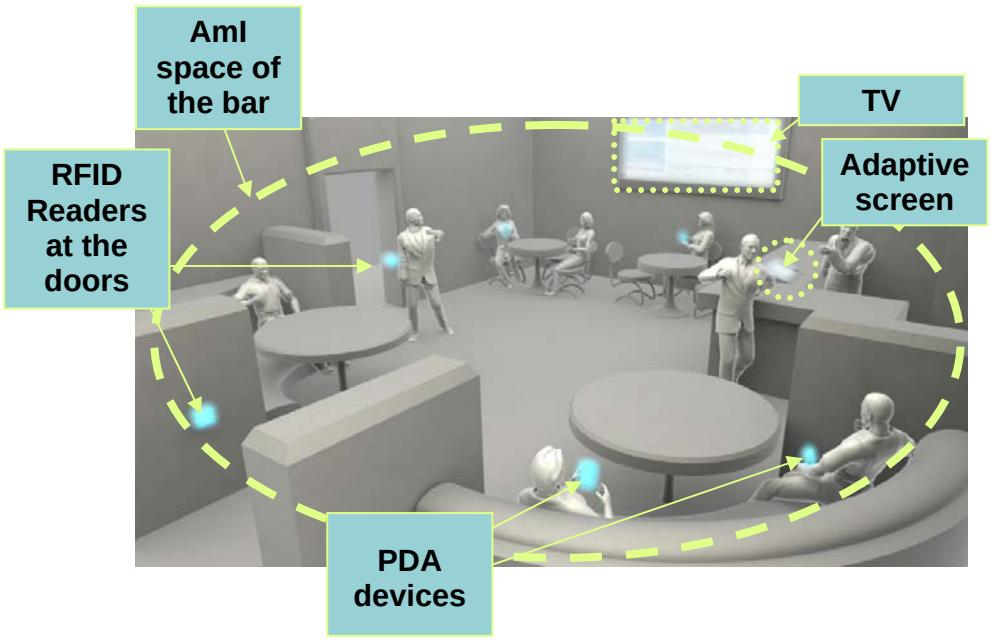


Figure 2-7: Possible future AmI space (Beslay et. al, 2005)

In this scene at a coffee bar, individuals are identified by means of either their PDA devices, or by implanted RFID tags. Personal profiles are mobile, such that people from outside of the local area can still have the same level of personalised service. When the individual enters the bar, they are identified and a personalised menu displayed to them.

This highlights some specific areas; firstly system architectures are needed to support portable wireless devices connected to and forming *ad hoc* fixed or wide area networks with distributed intelligence. However, from the mechanisms listed in section 2.1, the following are important for this scenario:

1. Function Identity-Administration
    - Communication-independent handling and representation of identities: Possibility to choose between different profiles if not correctly assigned by the AmI
2. Function Control
    - Rule-Handling performed by pre-editing the profile if inadequately assigned by the AmI
3. Privacy
    - The user must have ultimate control over which information is disclosed and to whom and the information utilised only by authorised devices. Notably, RFID tags have no method by which their access can be controlled and are thus potentially privacy violating
4. Security

- The AmI environment must provide efficient and reliable mechanisms to ensure data protection during both transfer and storage

5. Interoperability and Gateway
    a. The Identity information (i.e. personal profile) needs to be portable and understandable by any device, thus the first area of concern is that of seamless interoperability

2.7 Object identification in mobile computing

Identification is a central concept in mobile and ubiquitous computing, especially identification between electronic devices. While some applications require some kind of identification in the sense of authentication, e.g. for delivering authenticated data like sensor information, the paradigm of object identification is most useful for applications such as asset tracking (e.g. libraries, animals), automated inventory and stock-keeping, toll collecting and similar tasks where physical objects are involved and the gap between the physical and the virtual world must be bridged. In a world of ubiquitous computing, unobtrusive object identification enables the seamless connection between real-world artefacts and their virtual representations.

The security of the used identification schemes is crucial for mobile Systems depending on digital identities. An impressive example is an airplane which is normally identified electronically by a so-called friend-or-foe identification system (IFF). In this case, it is not the plane that is identified, rather its digital representation. Another example is, when identifying a PDA or mobile phone, common identification schemes can be bypassed by faithfully relaying all messages between the participating devices.

These kind of attacks are called mafia frauds and will be focussed on in this section. The best way of illustrating the mafia fraud and the corresponding problem known in the cryptographic community as *Chess Grandmaster Problem* is by telling the *famous story of the little girl who played ... against two Chess Grandmasters ... How was it possible to win one of the games? Anne-Louise played Black against Spassky. White against Fisher. Spassky moved first and Ann-Louise just copied his move as the first move of her game against Fisher, then copied Fisher's replay as her own reply to Spassky's first move and so on.*

Beth and Desmedt have already observed in (Beth and Desmedt, 1990) that mafia frauds cannot be prevented *only* by using cryptographic mechanisms. In particular, these mechanisms only prove the identity of the end-point of the communication, but give no hint *where* it is. Thus it is impossible to detect whether the expected end-point gives the answer himself or by (ab)using a third party. On one hand, this restriction is harmless as long as the exact position of the end-point is not relevant (e.g., by opening an encrypted communication channel to a logical object). On the other hand, this property is significant whenever the identification aspect comes to the fore, e.g., if a physical object has to be identified.

2.7.1 Solutions: An Overview

Faraday Cage. Bengio et al. (Bengio, Brassard, Desmedt, Goutier and Quisquater, 1991) suggest to prevent mafia frauds by isolating the object to be identified, e.g., by a Faraday cage. A Faraday cage electromagnetically isolates the device which prevents that a dummy device can communicate with another party. Two scenarios are conceivable.

The user and the device together enter some kind of secure room to perform the identification. This requires a trustworthy infrastructure of secure rooms which sounds expensive and

uncomfortable, but if, e.g., banks would make their ATM rooms secure (which, by the way, would also make the use of ATMs more secure), users could use them to identify their devices. The coverage of these rooms would be high (at least in cities) and users have to trust their bank anyway.

Second, the Faraday cage could be a part of a secure device (not the personal token; more looking like a microwave where you can put the device into) which performs device identification. The identifying device has to be trusted by the user, thus it should be owned by the user or a trusted party. The security benefit of separated Faraday cage devices is marginal. It only makes the mobile device as trustworthy as a stationary one, because the identifying Faraday cage device at home is protected by the same mechanisms (e.g., locks).

This solution also seems to be very unhandy and costly and does not solve the problem of device identification if the user is out on business or holiday where the identifying device is not available.

Channel Hopping. In (Alkassar and Stüble, 2002; Alkassar, Sadeghi and Stüble, 2003) a solution is introduced that is based on channel hopping technology and that is resistant against mafia frauds. The basic idea is that adversaries are unable to perform a mafia fraud if they cannot eavesdrop the messages send between identifying and the identified party. The solution is to partition the response of an ordinary challenge-response protocol and sent it over random channels of a large number of channels in such a way that only the owner of a secret key is able to receive the response.

The analysis shows that current FHSS (Spread Spectrum Frequency Hopping) technology with over 10^9 different channels and bandwidths of over 100MHz make mafia frauds very difficult and expensive. Modern DDS (Direct Digital Synthesizer) technology with an on chip D/A converter are small and power saving enough to be integrated into mobile devices.

Complexity. A more general solution of the channel hopping approach is to exploit the limited bandwidth that is available to the adversary. For a meaningful mafia fraud attack adversaries have to use wireless connections between original device and dummy. This limits the maximum bandwidth, because of size and speed of required transmitters and signal processing units.

In contrast, users who want to identify their device have direct access and are not subject to this restriction. Therefore, by using an identification protocol with a bandwidth that is higher than those of wireless connections, mafia frauds can be prevented.

By using, e.g., an optical connection between token and device for identification purposes allows the use of a very high transmission capacity between 10Gbit/s (multi-mode cable), 100Gbit/s (mono-mode cable) and 1Tbit/s (multiplex systems). Transmitting the information over conventional, non-directed (the adversary cannot predict the exact location and position of the device required for directed connections) wireless connection is very expensive or even impossible (UWB, Ultra Wideband Technology has a maximum transfer rate of 100Mbit/s). An example scenario would be a key fob with an optical interface, e.g., a laser diode, which is pressed onto the appropriate interface of the device to perform the identification protocol.

Distance Bounding. Instead of preventing mafia frauds, one can limit their applications by additionally ensuring that the identified device is close to the identifying user. Two different solutions have been proposed so far.

The first one, suggested by Desmedt et al., calculates the distance between device and user by comparing their absolute positions. The location can, for example, be derived from GSM cell or GPS signals (Desmedt, 1988; Denning and MacDoran, 1996). The device measures its position, signs the value with its private key and sends the signed location to the user which also has to measure its position, test the signature and compare the positions using an additionally required device. Problems of these approaches are their inaccurateness and that a trusted environment (the GPS or GSM signals) is required which can be fooled or disturbed using ECM (Electronic Counter Measures) mechanisms.

The second approach only calculates the relative distance between two parties using so-called distance bounding protocols (Beth and Desmedt, 1990; Brands and Chaum, 1994). This protocols measure the transmission time of messages send between two devices and derive their distance based on the constant speed of light. To get results that are precise enough very accuracy calculations are required which makes implementations very expensive. Additionally, the conversion into wireless transmissions are, compared with the delay, very large, which requires that also the conversion is performed very fast and therefore very expensive. For secure device identification, it has to be prevented that an adversary, e.g. sitting in the next room, can perform a mafia fraud attack, thus the granularity of the distance-bounding protocol should at least be 1m. Using a wired connection between token and device increases the delay of a wireless connection because of the latency of the converter.

2.7.2 Outlook

Object identification is a crucial task wherever physical entities have to be identified. An interesting case is the identification of humans, which usually is related to biometrics. However, the question is: How can we build biometrical identification systems that cannot be deceived be a mafia fraud? Our further research will also be marked by building up test beds for Channel-Hopping based solutions.

2.8 Linking a physical person with its digital identity

Identity management systems (IMS) manage digital identities, authorisations and rights of the identities and the delivery of services and credentials to their legitimate users. For a proper operation one needs mechanisms that guarantee that the digital identity represents the legitimate physical user (see requirement IV.b of section 2.1: Integrity of idenetity credentials). Today's main threat to the security of IMS comes from impostors who usurp a digital identity from a legitimate user (Phishing, social engineering, man-in-the-middle and other forms of identity theft). It is uncontested that Passwords or PIN-codes alone provide an insufficient tie between a physical person and its digital identity (Girard and Hirst, 2004). Stronger authentication schemes are mandatory for all IMS that manage valuable rights, data and services.

There are three different concepts to establish a link between a physical person and its digitally represented identity: Something that the person carries with her (token, like a smart card); something that the person knows (password, PIN-code); something that the person is (biometric feature). To authenticate a person one or more of such credentials based on these basic concepts have to be verified. Depending on the number of different types of such credentials one speaks of a one-, two- or three-factor authentication. It is important to notice that the only mean to establish a negative authentication (proof that an impostor tries to acquire a digital identity) needs a biometric factor.

Fig 2-8: Identity verification factors that can be used in an authentication process to link a physical person with a digital identity

2.8.1 Authentication within a Mobile Identity Management System

In all identity management systems (IMS) the set up of a safe link between a person and its digital identity is the most crucial process for the security of the whole access and authorisation chain. IMS use one or more of the three above mentioned concepts when an access requesting person has to deliver proofs for her correct identity. There are two different approaches for an authentication in an environment with mobile users.

- Centralised management of the authentication process for all users. The mobile device serves to transmit identity data provided by the user that will be evaluated against centrally stored authentication information about the user.
- Distributed management of the authentication process for all users. The mobile personal device contains the authentication data. No exchange or storage of authentication data with a central server is necessary. The mobile device delivers only information to proof that a secure link between the physical person and its digital identity has been established successfully.

In Mobile Identity Management Systems (MIMS) the authentication process is best implemented using the distributed concept to comply with the requirements I, II, IV, V, VI, IX and X listed in section 2.1. There are very limited possibilities to establish a secure and privacy protecting link between a person and its digital identity that includes biometrics by centralised mechanism. Such mechanisms always violate the requirements Ia, Ic, V, VI and X of section 2.1. Nevertheless many of today's IMS, even governmentally supported IMS, still rely on such centralised authentication concepts. The US immigration IMS with biometric registration of all foreign visitors and storage of these data in a centralised repository is probably the most prominent and intriguing example. There are also some critical points in a decentralised scheme. A distributed authentication process has to rely on the tamper resistance of the device that performs the mobile authentication (aMAD) and that delivers the appropriate identity proofs. As such devices are in the possession of the potential attacker

sufficiently high security standards for tamper resistance of the aMAD have to be requested, which in turn may have an impact on the price of the personal device. Although this may be a weaker point of distributed MIMS, its importance is limited. Even if a method to tamper an aMAD device is known, the malicious process can not be automated by a single attacker and the damage and therefore the interest of the attacker is always limited.

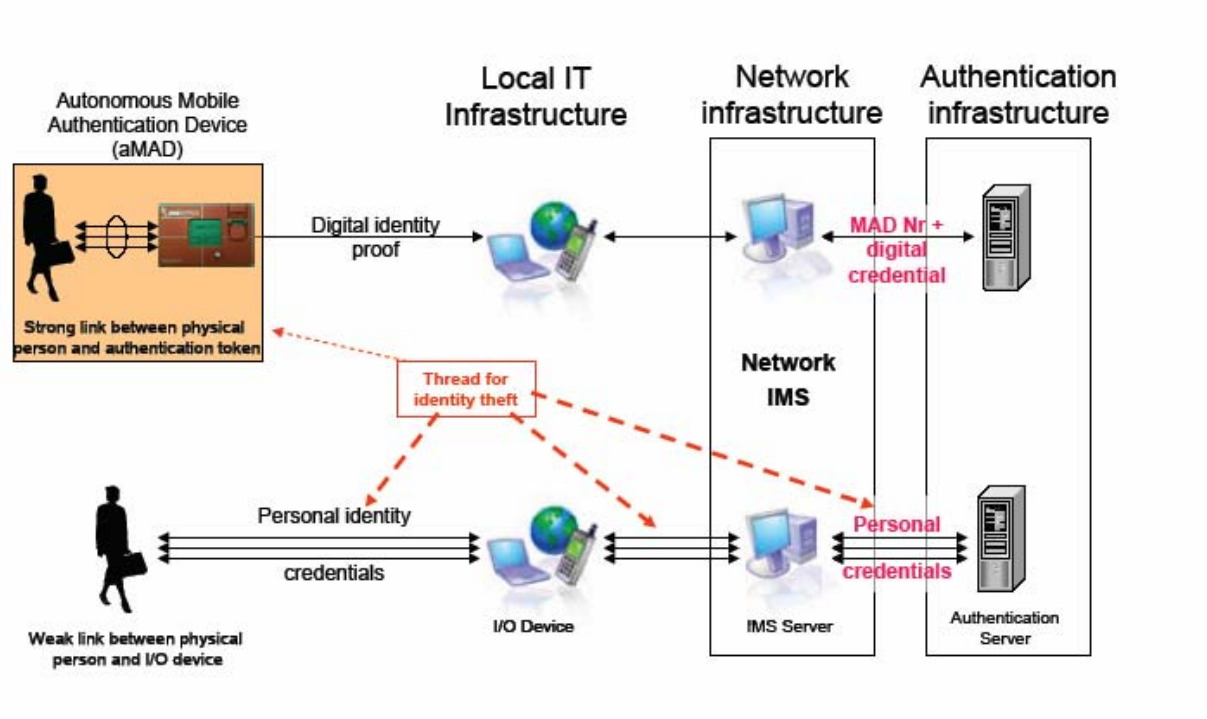


Fig 2-9: Flow of critical personal data in a identity management system with distributed and with centralised authentication

The centralised scheme has several drawbacks regarding security (many points of attack), privacy (central repository with critical information) and scalability (the separability of personal identity data diminishes with the rising number of users). There may be some advantages of a centralised scheme in the management of functionalities (requirements I, II), It is easier to update the evaluation of presented credentials or change credentials, when all relevant processing is centralised. The need to change evaluation protocols for credentials however is higher in a centralised scheme, as there is a greater risk of misuse at large scale.

2.8.2 Schemes for distributed 3-factor authentication

Far better than any centralised solution are distributed mechanisms that provide a secure link between physical persons and a digital identity certificate enclosed inside a personal mobile token. The token contains the necessary information to establish the link between the physical person and its digital identity without interaction with a centralised data repository. SIM-cards with a PIN authentication are an example of such a mechanism with two-factor identity verification. For many applications with higher security requirements or with the need for negative authentication a two factor verification mechanism without biometrics is no more acceptable. There are several concepts that allow a distributed three-factor authentication

- Smart cards that store a biometric matching template, acquired in the enrolment process which may be compared with a locally measured query template
- Smart cards that store the biometric matching template and the matching algorithm on the card (match-on-card, MOC)
- Tokens that provide the full biometric authentication process including the sensors and the feature extraction to acquire a query template from the biometric measurement (autonomous mobile authentication device, aMAD)

Only the last solution fulfils entirely the req. Ic, Vb and VI and IX. The availability of special hardware (biometric sensor equipment) at any authentication site is a serious restriction for the wide application of one of the two first mentioned solutions. Only the third scheme allows unrestricted mobility of the user, unlimited availability of the authentication procedure and full containment of all privacy critical biometric data inside the personal token. The last scheme allows the adoption of federated identities based on partial identity information provided by the mobile authentication token. This is important to fulfil the requirement of supporting federated identities as the interoperability of identity credentials is not guaranteed without a ubiquitous trusted PKI infrastructure. An aMAD-token may store many independent digital identity certificates to authenticate the user directly to different network IMS. The different network operators have only to trust the certification authority that edits the aMAD-tokens and the initial enrolment process. In chapter 5 a realisation of an aMAD is presented (AXS-ID-card).

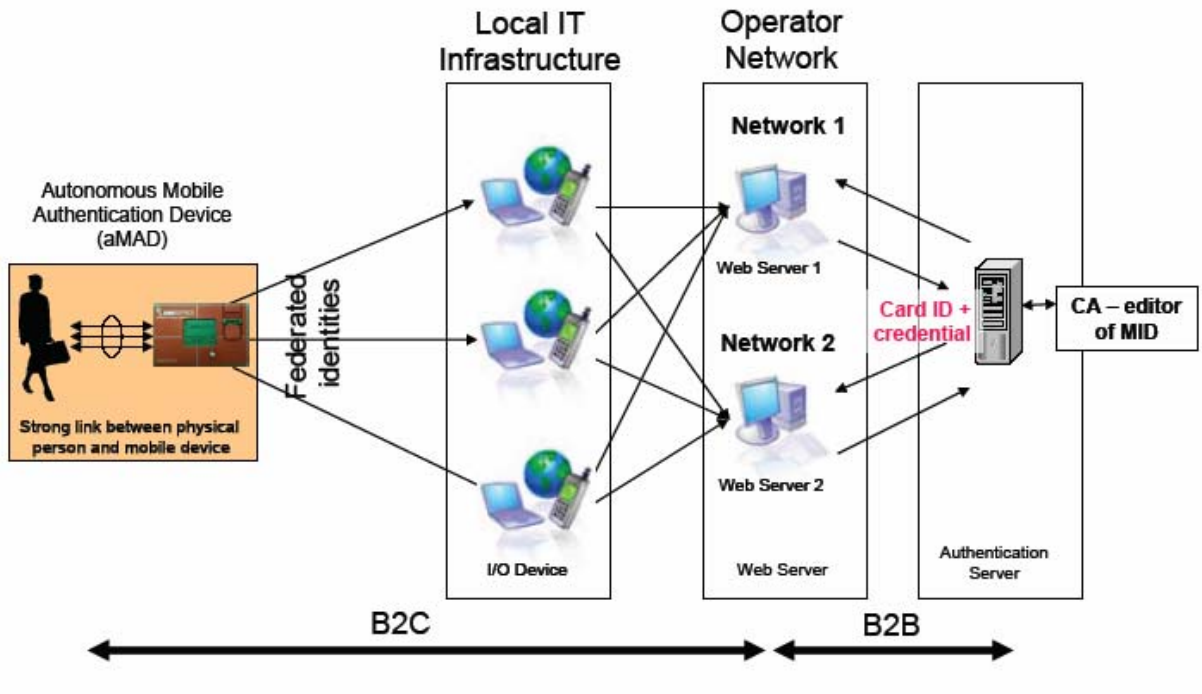


Fig. 2-10: Within a distributed authentication scheme federated identities are realised in a simple way by storing multiple identity certificates in one token

2.8.3 Digital identity proofs using the authentication token

There are several solutions for authentication tokens on the market: Smart Cards with electrical connection or RF-interface, OneTimePassword-Tokens, USB-Tokens, tokens in form of a cell-phone, PDA or Pager and SW-tokens to be loaded on a personal mobile computer. All the tokens contain a secret that can be verified by an external IMS operator or authentication service provider. The verification process between remote IMS and authentication token is only activated after a successful person-to-token authentication. There are three different concepts to use a secret in such tokens as identity credential:

- In a Challenge-Response-Protocol (CR) an external operator verifies that the token contains the secret through en encrypted transmission of a one-time password (OTP) into the token. The token decrypts the encoded message with the secret and delivers the OTP. The later presented AXS-ID-card works with a CR-protocol that allows additional services based on the same token.
- The token delivers an OTP generated simultaneously inside the token and on the authentication server. Both sides share a common secret and are time or event synchronised. The OTP changes on both sides simultaneously at a certain pulse rate
- The token generates a linear hash code combining a secret and a time stamp that can be verified on the operator side. The well-known SecureID of RSA works with this concept.

A common feature of all authentication tokens is that the base secret is completely independent of any personal identity information of the user. The observation of the secret exchange does, in no way, reveal any information about the identity of the user to a third party (unobservability).

3 Privacy for Mobile Users

This chapter describes privacy threats for mobile users. Alan F. Westin defines privacy as

"[Privacy is] the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" (Westin, 1967).

Based on this definition, privacy in this study is considered as the ability of a mobile user to control the disclosure of personal attributes towards his communication partners. Anonymity of a user is a requisite for privacy. The following attacker model for mobile users identifies the anonymity threats by an attacker who wants to trace and identify a mobile user. Privacy threats for mobile users in *ad hoc* networks are described by scenarios and by using services for personalising the user interface of a mobile device in WAP based systems.

3.1 Freiburg Privacy Diamond

The *Freiburg Privacy Diamond* (FPD) is a model that tries to capture the essence of anonymity with regard to the most important forms of mobility in mobile communications: device mobility and user mobility. It must consider therefore at least four types of entities: the action itself, the device used for the action, the user who performs the action and the location which the device and the user are located at.

The FPD (see figure 3-1) describes how these entities are related and how an attacker can use knowledge about these relationships to break anonymity. With this completely interconnected graph it is possible to describe which information can be concluded from other information. The use of the FPD is illustrated in a very simplified fashion by the following example:

An attacker attempting to disclose the identity of a user tries to reveal the relationship between the user and an action. To do this, he could find out which device was used for this action and then find out who used this device. If the identity of the device used for the transaction is concealed, e.g. using a mix network (Berthold, Federrath and Köpsell, 2001; Chaum, 1981) or crowds (Reiter and Rubin, 1998), this deduction is not possible. But it may also occur that the device and the location of the device are known, e.g. if the user goes to an Internet-Café. However, there is no *a priori* knowledge of the user of the device. This knowledge can only be gained, if the user reveals her or his identity directly.

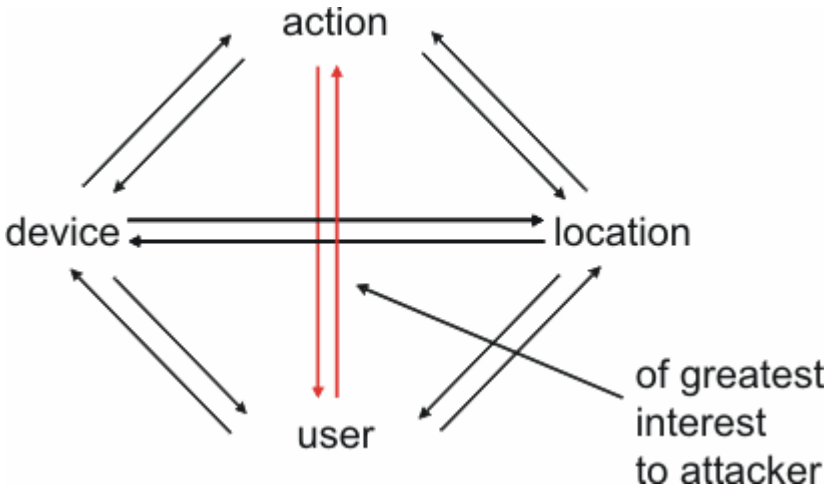


Figure 3-1: Attacker model for mobile users: Freiburg Privacy Diamond

3.1.1 Model Assumptions

The privacy diamond is used to represent the knowledge of the attacker in the following situation: a user operates a device at a certain location to initiate an action. Four entities are necessary to model the situation: the user, the action, the location and the device. These will be addressed below. Time will only be considered as an implicit parameter.

Mobile users use a device to perform actions. These actions are considered to be atomic; during an action neither the user, the device of the user nor the location of the user changes. The action is also instantaneous; it is carried out while the user uses the device. To model location information, the world is divided into cells. The size of these cells determines the maximum resolution to which a device or user can be located.

Users perform actions using a single device from a set of devices. The device is located at the same position as the user. This assumption is realistic as the user has to be in the proximity of the device to operate it.

The scope of the definition of the device includes all software on this device. If the software is able to migrate from device to device, like mobile agents, this node of the graph would have to be replaced by several nodes. This situation is not considered here.

3.1.2 Classes of Anonymity Mechanisms

Intuitively, there are five loop-free paths which can be used to deduce the identity of a user by linking this action to the user:

- user to action directly
- user via location to action
- user via device to action
- user via location and then device to action
- user via device and then location to action

For anonymising systems that are secure against an attacker calculating the transitive closure, all five paths have to be broken. There are four minimal ways of doing this (see figure 3-2),

leading to four classes of minimal anonymity mechanisms. Minimal means that it is not possible to re-connect a severed relation in the privacy diamond without allowing the attacker to infer the relation of user to action through transitive closure.

Anonymising mechanisms in the category described by the privacy diamond in figure 3-2a are those that do not require mobility, e.g Mixes (Berthold, Federrath and Köpsell, 2001; Chaum, 1981) and DC-nets (Chaum, 1988; Waidner and Pfitzmann, 2002). The privacy diamond in Figure 3-2b describes anonymising mechanisms that rely on user mobility like phone booths or Internet cafés. An anonymising mechanism in category c) relies on broadcasts to and from a specific device. Both categories b) and c) rely on the users changing their devices. Therefore, it is not possible to employ a personal device. Category d) requires terminal mobility, enabling users to use their own devices. It also permits the location of the action to be visible on the network, thus allowing optimisation of routing, etc. RFC 3041 (Narten and Draves, 2002) and location addressing are examples of mechanisms in that class.

It is possible for an anonymity mechanism to be contained in two classes if it is not minimal. This can happen by a combination of mechanisms of different classes. Relations that must be obscured by the anonymity mechanism are shown by dotted arrows.

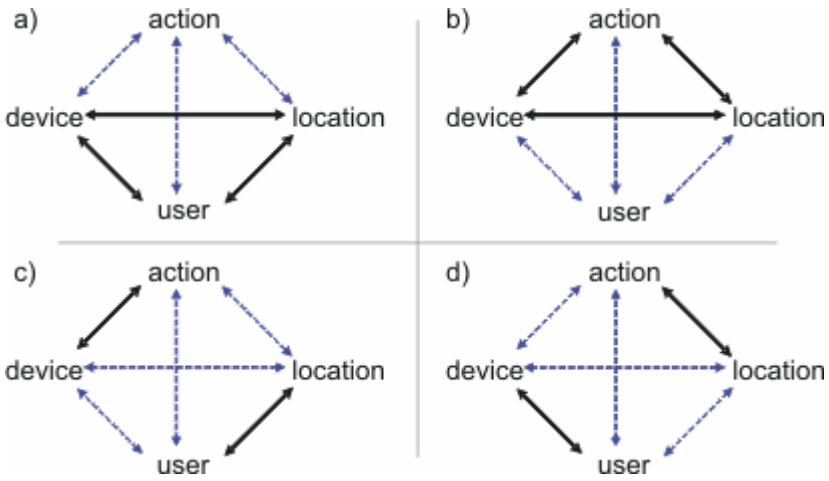


Figure 3-2: Four minimal possibilities for anonymity mechanisms

3.1.3 Summary

The *Freiburg Privacy Diamond* models the information processing of an attacker. It can be used to understand the impact of user and terminal mobility on anonymising systems. It can be seen that mobility offers new possibilities for designing anonymity mechanisms. This is important as new anonymising mechanisms are required that observe the constraints imposed by mobile communications systems.

By weighting the relations, it could be used to analyse anonymity mechanisms and provides a measure of the degree of anonymity and of the confidence that a specific user performed a certain action. For a real attacker, using this model to attack anonymity would have a major drawback. Since no exclusion of possibilities is possible in the model, the information being sought could get lost in the mass of inferences.

3.2 Privacy in mobile ad hoc Networks

3.2.1 Background

Mobile *ad hoc* networks can be defined as mobile platforms or nodes that can move freely and establish ephemera wireless networks without central entities to control it. At a first glance, mobile *ad hoc* networks may not seem directly related to mobile identity management. However, identity management does not necessarily imply a client-server structure where a user is communicating with a server. Also peer-to-peer scenarios in which users communicate directly with other users are of interest in the context of mobile identity management. As seen in the scenarios later described in this chapter, mobile *ad hoc* networks constitute a technical infrastructure that could provide a base for both traditional client-server applications as well as peer-to-peer applications.

Mobile *ad hoc* networks are a fundamental building block for ubiquitous computing (also referred as pervasive computing or ambient intelligence, see sections 2.6 and 2.7) and sensor networking, two major technologies that will have a great impact in several areas, such as environmental control, surveillance, advertisement, marketing, business modelling, etc. However, these two technologies will have a huge impact on privacy as they can be used to track people and also monitor their behaviour. A general definition for ubiquitous computing is a computing infrastructure for getting information everywhere, at any time, being accessed through invisible interfaces. Instead of data being input via conventional interfaces such as a keyboard or a mouse, it enters the system via ubiquitous sensors in the user's environment. Ubiquitous computing has a large spectrum of potential applications and highly futuristic fully networked environments can be imagined. Sensor networks are a special kind of computer networks composed of several nodes that communicate using wireless interfaces and are spread in a determined geographical area. They have as goal to collect environmental information through embedded sensors and transmit it back to one or more computers, called sinks. Sensor network applications include among others: environmental data acquisition, surveillance and embedded sensors in vehicles, for instance.

As discussed above, these new technologies make promises of revolutionary applications that may change our way of living. However, the other side of the coin is that these technologies can harm people's privacy. Mobile *ad hoc* networks, sensor networks and ubiquitous computing can be used for tracking people and their habits. In addition, profiles can be built with the acquired data and real big brother scenarios can be foreseen.

3.2.2 Introduction to scenarios

The concept of mobile ad hoc networks provides many challenges to privacy. Vast amounts of potentially sensitive data are being transmitted among the mobile devices in the network, where some of these data may be highly sensitive data about for example the owners of the devices.

In order to illustrate different potential privacy problems in the mobile *ad hoc* domain, two different usage scenarios have been defined. In the first scenario (the mobile Internet scenario) a user (called John Smith in the scenarios) in a mobile *ad hoc* domain makes use of services on the mobile Internet through the mobile *ad hoc* network. In the second scenario (the intra *ad hoc* scenario) the user Jim wants to communicate to another user within the mobile *ad hoc* network.

These scenarios are presented in two different versions; firstly one version where privacy problems have not been fully considered and secondly one "privacy-enhanced" version where the privacy needs of the user are embraced. The initial version of the scenarios is used to illustrate a number of imaginable privacy problems for the user. In the second version of the scenarios, anonymity technologies are introduced in the technical environment as a countermeasure to these privacy problems. These technical solutions aim at providing anonymity for the users by offering non-linkability of transactions. Thus, this section does not describe a full-fledged identity management solution. However, in order to offer identity management applications, anonymity is needed as an underlying base. The technical solution presented in this section could provide a base for a more advanced identity management application.

3.2.3 Initial usage scenarios

Scenario one – the mobile Internet Scenario

In this scenario John Smith is visiting a pub in an area often populated by people interested in new technologies. At the pub, John is participating in a mobile *ad hoc* network to which he is connected via his new mobile phone. Using Mobile IPv4, John is also connected to the mobile Internet via the mobile *ad hoc* domain. John is downloading streaming video from a WAP server on the mobile Internet which he views on his mobile phone. Since John is interested in stocks, he is downloading video material teaching him how to be a successful man on the stock market.

Scenario two – the intra *ad hoc* Scenario

In the second scenario John feels a bit lonely. Since the pub is crowded with people, he uses his mobile telephone to find out if any of the people in the pub are using "Instant Mobile Dating", a popular mobile dating application in this scenario. When going online, he immediately finds a matching profile in the pub and therefore spontaneously initiates a chat session. John and his chatting partner share many similar interests and after some minutes of virtual conversation, they decide that they have built up enough mutual trust to join tables and continue their discussion in person.

3.2.4 Privacy problems in the scenarios

There are many concerns for privacy in the scenarios described above. In the first scenario John feels a bit uneasy about letting other people know about his interest in the stock market. He is a bit worried that someone would use this knowledge to deduce that John is a wealthy man and therefore follow him and later rob him. Also, John does not really trust the company hosting the video streams that he is downloading. John fears that the company will gather profile information about him and later possibly sell this information to other companies so that he will eventually be flooded with vast amount of unwanted commercial information.

In the second scenario, John also worries about his privacy. He does not want other people at the pub to know that he is feeling lonely and depressed. Therefore he does not want other people to know that he is participating in the mobile dating service. Also, he is a bit afraid that his chatting partners at the pub may be pranksters that will figure out the identity and physical location of John and then make fun out of him. John wants to be completely anonymous when using the dating application until John himself decides otherwise.

One additional issue also concerns John - the issue of location privacy. In MobileIP, the concept of a home agent is used to allow users to be reachable when they are travelling to other locations, like John is doing in the scenarios. The home agent (often operated by the Internet service provider) is a static part of the infrastructure that always keeps track of the user's whereabouts when roaming. It has been pointed out that location data within this kind of traffic data, even though it is less precise, can also contain sensitive information about the "relative positioning" and "co-located displacements" of mobile nodes and thus also require special protection (Escudero-Pascual, Holleboom and Fischer-Hübner, 2002). The home agents in mobile nodes' home networks keep track of the mobile nodes' care-of addresses in order to tunnel datagrams for delivery to the mobile nodes when they are away from home. They are thus critical aggregation points that can possibly store and compare communication profiles of mobile nodes. Thus, John's home agent is building up a user profile of John that includes his travelling habits. John is concerned by this and he want to be able to roam among different foreign networks without being constantly localised by his Internet service provider (or whatever entity that operates the home agent). The issue of locations privacy are dealt with separately in section 3.2.6.

3.2.5 Privacy-enhanced usage scenarios

Scenario three – privacy-enhanced Internet scenario

Based on the discussion in the previous section, the privacy-enhanced version of the mobile Internet scenario aims at (1) stopping other visitors at the pub eavesdropping on the communication between John and the WAP server and (2) hinder the WAP server to pool information about John in order to create an extensive user profile about him and to trace John's locations.

To address the privacy problems mentioned above, John and other visitors at the pub are jointly participating in an anonymous overlay network that resides on top of the existing mobile *ad hoc* network. An overlay network is a virtual network of nodes and logical links which is built on top of an existing network and which implements network services not available in the existing network. In this case, the purpose of the anonymous overlay network is to provide anonymous communication for the members of the network. Since static infrastructure is not available in *ad hoc* networks, every member in the overlay network constitutes of a node in the network themselves and communication is routed along these nodes according to the rules of the protocol in the overlay network. The logical links along which the communication in the overlay network is routed are called 'virtual paths'. If John now downloads streaming media from the WAP server on the traditional Internet, as described in the first scenario, neither outsiders (people at the pub not participating in the anonymous network) nor insiders (participants of the anonymous network) can learn the fact that it is John that is downloading the streaming media.

In figure 3-3 below, the privacy-enhanced version of the mobile Internet scenario is illustrated. The numbers in the figure 3-3 corresponds to the members of the anonymous network. Since MobileIP v4 is used to interconnect the mobile *ad hoc* domain and the wired domain, each member has a home agent residing at his home link / network. When John (the user denoted "3" in the figure 3-3) communicates with the WAP server, the communication is first routed along the virtual path in the left part of figure 1 that was built up in the anonymous overlay network for this session. Then, after passing the access point (denoted AP) and the foreign agent (denoted FA), the request eventually reaches the WAP server. On the way back, the reply also passes the home agent of the last node in the virtual path

(denoted HA4). This is necessary in order to find the foreign network hosting the mobile *ad hoc* network.

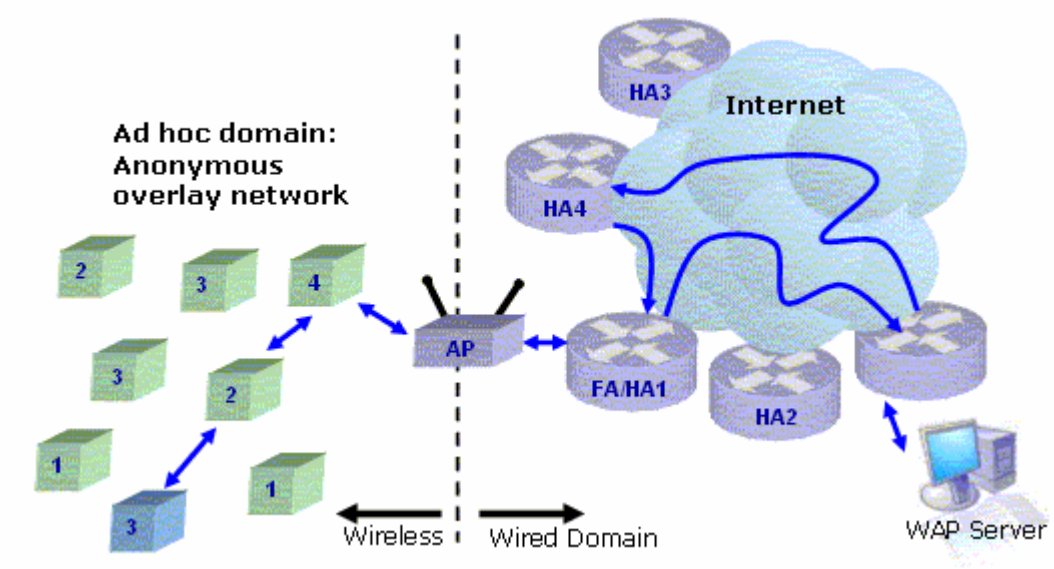


Figure 3-3: The privacy-enhanced Internet scenario

Scenario four – privacy-enhanced intra ad hoc scenario

The goal of the privacy-enhanced version of the intra *ad hoc* scenario is to (1) stop other participants in the mobile *ad hoc* network learning that John is using a mobile dating server and (2) stop them from knowing with whom he is communicating. Furthermore, (3) he wants to be anonymous against his chat partner until he decides the level of mutual trust is high enough to reveal his identity.

To fulfil these privacy needs, John participates in the same anonymous overlay network as the one described above in the privacy-enhanced mobile Internet scenario. Figure 3-4 below illustrates the privacy-enhanced version of the intra *ad hoc* scenario. In this figure, the node "J" represents John and the node "C" represents his chatting partner. Besides guaranteeing anonymity towards his chatting partner, John also has the possibility to be anonymous towards both outsiders and insiders.

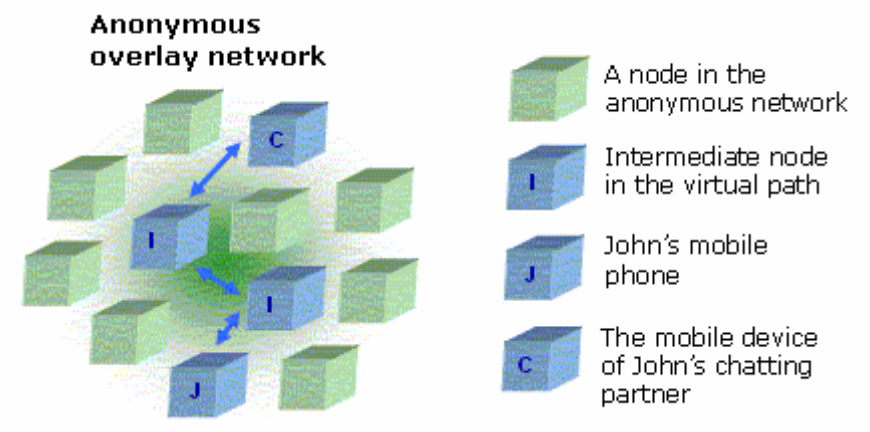


Figure 3-4: The privacy-enhanced intra ad hoc scenario

3.2.6 Ensuring location privacy in mobile ad hoc networks

If John does not want the home agent to know about his location in the first scenario, some additional technical means to protect location privacy have to been introduced in the wired domain. It is not possible to solve the location privacy problem in the mobile *ad hoc* domain, since the problem originates from the concept of the home agents in MobileIP. One possible solution is to combine the anonymous overlay network in the mobile *ad hoc* domain with an Internet-based solution that protects location data in MobileIP.

One solution is the Flying Freedom System (Escudero-Pascual, Heidenfalk and Heselius, 2001), where a set of protected extensions in the mix-based Freedom System architecture were introduced to permit a mobile node to seamlessly roam among IP subnetworks and media types while remaining untraceable and pseudonymous. This solution is illustrated in figure 3-5 below. Now, when a user is roaming among different foreign networks, the home agent only knows that it is forwarding messages to the Flying Freedom server (FF in the figure). After passing an anonymous communication network based on Chaumian Mixes, the request is eventually forwarded to the foreign agent (denoted FA).

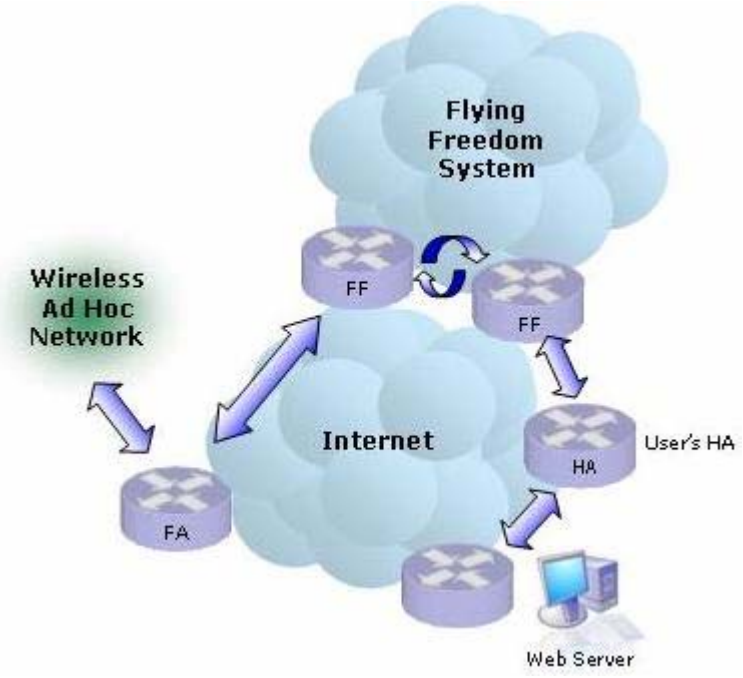


Figure 3-5: Using the Flying Freedom System to achieve location privacy

Finally, another (probably more ungainly) solution would be to require the user to operate his / her own home agent that is under his / her own control.

3.2.7 Future Work

New developments of anonymity technologies are needed to adapt existing solutions to the new challenging area of mobile *ad hoc* networks. For example, the scenarios assumed a sound anonymous overlay network in the mobile *ad hoc* domain that both provides strong anonymity and fits the characteristics of mobile *ad hoc* networks. A number of solutions for

anonymous communication on the traditional Internet already exist today, such as Chaumian Mixes (Chaum, 1981), Crowds (Reiter and Rubin, 1997) and Tor (Dingledine, Mathewson and Syverson, 2004). However the special nature of mobile *ad hoc* network makes these anonymity technologies infeasible (see section 5.3). Even peer-to-peer based solutions like Tarzan (Freedman and Morris, 2002) and MorphMix (Rennhard and Platter, 2002) do not fully meet the requirements for mobile *ad hoc* networks. Thus, in order to guarantee privacy in mobile *ad hoc* networks, new anonymity technologies have to be developed that fully meets the needs for mobile *ad hoc* network environments or existing ones need to be updated. Karlstad University is currently developing an anonymous overlay network suited for mobile *ad hoc* networks.

3.3 Privacy Risk of User Agent Systems in WAP based Systems

Well-known privacy problems of the traditional Internet, as caused by cookies, customer and communication profiling or SPAM, are also issues in the mobile Internet. One of the major new privacy problems introduced by mobile Internet architectures is the problem of location privacy. Data about the precise geographic location of the user (or more precisely user device) are perceived as sensitive and therefore according to Art.9 EU Directive 2002/58/EC need special protection.

In addition to location data, further kinds of personal data are needed in the mobile Internet environments for personalisation, content adaptation to minimising performance costs as well as for context-aware services. In the mobile Internet, where restricted devices with small screens are in use, personalisation is a much bigger issue than in the traditional Internet, where personalisation of sites is rather a matter of convenience to the end user.

Information about the device capabilities and user's preferences in so called User Agent Profiles can be especially useful to allow the service provider to generate content tailored to the characteristics and user interface of the requesting device and thus enhance the mobile user's experience and minimise the use of bandwidth. The Composite Capabilities/Preference Profile (or short: CC/PP) recommendation (CC/PP) by W3C specifies how a client side user agent, such as web browser in a PC or a mobile phone, can deliver a description of its capabilities and user's settings to a content server. The User-Agent Profile (or short: UAProf) Drafting Committee of the WAP Forum (now: Mobile Internet Alliance) created a specification (UAProf) based on the original CC/PP note (CC/PP Note 1999) including some WAP specific extensions. CC/PP allows origin servers to generate content that is adapted to the requesting user agent and the user's preferences by sending Capabilities and Preference Information (CPI) within an HTTP or WSP request to the origin server. CPI is represented by means of a profile, which comprises a set of components. In UAProf, these include hardware platform, software platform, network characteristics and personal settings. The UAProf specification also defines location as a reserved attribute. Profile Unified Resource Identifiers (URI) are sent using the profile header inside the HTTP request. The URI refers to the location of the profile in a profile repository. Intermediate network entities may optionally add content transforming capabilities or location information to the profile by adding a special header called Profile-diff, devoted to the purpose of conveying single or few attributes.

CPI in User Agent Profiles also comprises personal data about the device holders, which if used in a certain context or for a certain purpose can become very sensitive. For instance, the information that someone has a very expensive mobile device could be used by mobile marketing services to provide more exclusive and expensive offers and could in combination

with the user's location data also be of special interest to burglars. The fact that a user is choosing settings for larger letters or voice only could lead to the conclusion that the user is visually handicapped. In (Nilsson, Lindskog and Fischer-Hübner 2001; Fischer-Hübner, Nilsson and Lindskog 2002) privacy problems of capability and preference information are discussed. CPI in user agent profiles is therefore also part of a mobile user's identity and the mobile users needs to have the possibility be in control over it.

In (Fischer-Hübner, Nilsson and Lindskog 2002), results of the PiMI prototype project with participants from Ericsson AB and Karlstad University are presented. In the PiMI project a browser built-in and a proxy-based P3P (P3P) user agent for controlling the dissemination of CPI in mobile Internet environments by the means of Minimal Profile Conveyance was developed. The approach of Minimal Profile Conveyance requires that the user defines a minimal CPI profile, containing only information that the user considers completely harmless, or where there is an understanding that this information may be necessary for some reason. In the extreme case, the profile could be empty. This minimal profile can be used:

- for accessing non-P3P enabled web sites or web sites that do not meet the user's P3P privacy preferences
- for serving third party requests to the WAP Gateway for cached profiles (such as for WAP push content generation)
- for communication in the "safe-zone" (as defined in P3P) before a P3P agreement

The end user also has to define a full CPI profile to be used when there is a successful P3P agreement, i.e. the site is P3P compatible and the site's P3P policy file matches the end user's privacy preferences.

Even though P3P can enhance transparency and control over data disclosure for users, it has also been criticised as it does not ensure compliance of privacy policies with privacy laws, it does not guarantee a minimum and non-negotiable level of privacy protection for individuals and in its current form it does not fulfil the legal requirements for obtaining technically user consent.

Privacy-enhanced mobile identity management systems can go a step further and should provide a means for privacy control (consent, objection, disclosure, correction, deletion and addition) and for privacy-compliant data processing of CPI and other personal data belonging to a user's mobile identity.

4 Usability and Security for Mobile Identity Management Systems

The security of a system vastly depends on the willingness of the user to use security mechanisms (Waidner, 1998; Whitten and Tygar, 1999). Users underestimate the consequences of insufficient security. Thus they are not willing to invest a lot of effort in order to learn how to use these security mechanisms (Müller and Stapf, 1998). It can be shown that the main reason for this is the incomprehensible presentation of the security mechanisms and not the ergonomic design of their user interface (Müller and Stapf, 1998; Gerd tom Markotten and Kaiser, 2000). For example, the evaluation of the security software "SignTrust Mail", developed by the Deutsche Post AG, has identified 120 usability problems. 89% of these identified problems have a negative effect of the system's security (Gerd tom Markotten, 2004). Thus a test person could not reach his protection goals and broke his task off. 75% of the test persons did not understand asymmetric cryptography and therefore could not use it correctly.

A solution is self-explanation, where two options can be followed (Simon, 1957; Balfanz, 2003). Either one develops new user-consistent metaphors or one hides security from the user altogether. The first option will be addressed by style guides to enhance the user interface and by testing security tools in order to ascertain its comprehensibility and integration. The limits for the second option have been laid by analysing the interdependency of protection goals, discovered and classified in multilateral security (Jendricke and Gerd tom Markotten, 2000). The differentiation into system-controlled and user-controlled protection goals is shown in figure 4-1. Only user-controlled protection goals and mechanisms cannot be automated while system-controlled protection goals can be hidden from the user interface.

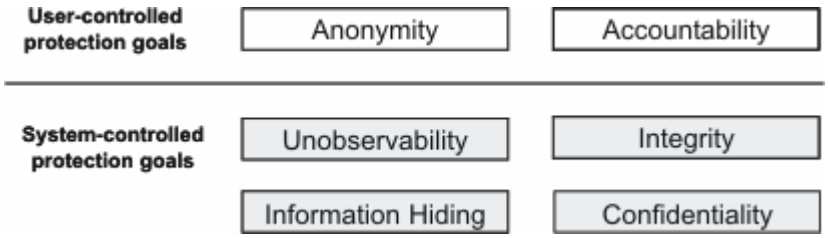


Figure 4-1: Implications of Protection Goals

In the following section results on studies on P3P for mobile phones will be described as an example of the usability of security tools for mobile devices. The ongoing research on usability of identity management systems for the mobile user will be introduced by identity management mock-ups for mobile phones.

4.1 *Studies on Usability of P3P for Mobile Phones*

4.1.1 Alerting and Informing in P3P Enabled Browsing

P3P, W3C's Platform for Privacy Preferences Project, defines a set of terms that Internet service providers can use to describe their privacy practices in both a standardised, machine-readable way and also in a human-readable way. This enables users to understand what data

will be collected by sites they visit and how that data will be used. (Cranor, 2002) The latest draft of the P3P element definitions can be found at P3P's web site (P3P, 2003).

If users are able to rely on user agents performing some or most of the analysing of web and WAP sites' policy statements, then there must be a swift way of telling the users the results of the analyses. In some P3P-enabled web browsers the user can set the conditions for when the agent shall give a warning (alternatively this could be used to block access in the way the PICS classification is used). In general, one could imagine two kinds of conditions for warning: either the site does not contain any P3P policy statement at all, or there is such a statement but it deviates from the user's preferences. In either case a warning should be given and in the latter case the agent should display the deviating declarations either automatically or upon request from the user. It should be noted that the user may not be worried by a warning when he enters certain kinds of trusted sites, such as his local hospital, even if their policy statements tell about far-reaching uses of information which are directly linked to him.

In our studies, the focus has been so far on textual rather than voice presentation. It has not been assumed that users will use earpieces or phones with free speech capabilities to hear alerts or to listen to the information of the privacy preference setting pages. Certainly, other kinds of alerts are possible when using an ordinary mobile phone, especially using the ringer signal, vibration and the LED indicator. However, using a ringer signal makes it impractical to use WAP at many public places and shared work places (compare desktop computers environments where the sound level can be set once and for all, which makes the user familiar with the sound of the alert signal). Vibrations and LED indicators are not present on every model of mobile phones. Furthermore, LED indicators might furthermore not be immediately visible for persons using the WAP function of their phones. Concentrating on on-screen information makes it possible to compare the merits of different display sizes.

Preliminary prototypes have concerned phones models with different screen sizes; the smallest being 100 x 80 pixels. Only one test subject used this prototype because it was not successful at all. This person did not notice when the alert symbols were switched on, or the icons got in the way for the ordinary text or disappeared. Alerting in devices with the smallest screens will possibly have to including ringer and vibration. However, one should also rethink the alerting needs. Simple browsing should not cause any alarm regardless of the privacy policies of the visited sites, because the browser should simply be anonymised and not give away any information about itself or its user if no anonymisation is used. In fact, because many sites are not P3P-enabled a warning will have to be given very frequently. The resulting frequent interruptions may not be wanted and neither would it be easy to inform the user of what the different policy details in effect mean on-the-fly.

4.1.2 Setting privacy preferences

In addition to the alerting function, there should also be a function allowing a user to set his privacy preferences. If users are supposed to be informed about how personally identifiable data are used, then there should be a way of setting such preferences in an informed way. Users have to be able to understand the alternatives when setting their preferences. Informing the user at this stage could be pursued in various depths depending on what the user requests. Because the screen size is limited one has to structure the information in accordance with limitations of people's short-term memory capacity. Scrollable pages might be a good solution; because vocabulary tests (see below) had indicated that many users are not familiar with privacy terminology, it was decided to use a design with hyperlinks in the privacy setting menu. Brief tests with hierarchical screen-sized pages with text-links between levels have

been made. Links could be clicked by the users to get a definition or explanation of specific terms, or to get to a page with a menu allowing the user to set option for the personal definition. For instance, if the user clicked on "sensitive information", a screen appeared which allowed the user to define what sensitive information is for him.

4.1.3 Vocabulary tests

The Internet is used by people of varying linguistic backgrounds. This may cause problems if users are to exercise informational self-determinacy based on privacy policy documents in the language of the web site owner only. W3C's Platform for Privacy Preferences Project, P3P, designs a set of tags to enable automatic interpretations of privacy policies of web sites. The tags have short but comprehensive definitions in the English language, but these definitions are too technical to be readily intelligible for lay English users. The P3P has therefore suggested a set of simplified phrasings in the English language (P3P, 2003). They call these simplifications 'translations'. However, one might avoid using this word in that sense when discussing inter-linguistic issues where the word 'translation' already has an established meaning. Non-English users' understanding of privacy vocabulary has been the topic of investigation below.

For instance, when twenty-four Swedish first-year students were given a questionnaire (a few weeks after the academic year had started), the results showed a rather weak understanding of frequently used terms. The *opt-in/opt-out* options might seem essential to any use of network services, yet only two persons tried to explain the meaning of these concepts. What is more, their answers do not reveal any real insight into the matter: "In-option and out-option" might be based on some experience of these options but might as well not, while "Optical in or out" is definitively wrong. The word *consent* is not specifically used within computer-related fields and could supposedly be understood by any university student. Nevertheless, 80% said they did not know its meaning.

4.2 Identity Management Mock-ups for Mobile Phones

The problems encountered while adjusting the PRIME mock-ups made for computer screens to mobile phones have to do with the mobile's smaller screen. It could easily cause the user to lose sight over the program. For the mock-ups an Ericsson P900 was used, which has a 208x320 pixel screen which measures 4 x 4 cm folded and 4 x 6.1 cm unfolded. This is a large screen in comparison to, for example, the T610 which has a 128x160 pixel screen, but is still smaller than a PDA (Personal Digital Assistant, e.g. PalmPilot).

From a user's perspective the identity management (IDM) function might be quite secondary to the task the user tries to perform, but there is a risk that 'full' IDM windows cover the entire screen (menus for example, see Figure 4-2). A comprehensive presentation of IDM controls will hide the other controls and also hide system feedback that might be relevant and even necessary for the user to understand what he is doing.

The mock-ups were constructed to explore graphically how severe this problem may be and to visualise possible remedies. The interaction elements designed for the PRIME web user interfaces were used, but because of the lack of room, some information texts were shortened. Hyper linking and scrolling was also suggested in the mock-ups. This way the texts are not visible in total but the user may be less disoriented.

Figure 4-2: The PRIME menu in a 4 cm x 6 cm display

Preference settings form: all information cannot be shown in the same window but this may not be very detrimental if users utilise a desktop computer to make the preliminary settings.

Browser view: not much information can be given simultaneously with the browser window; there is very little room in the browser to show both the preference set's icon or name and an intelligible indication of the present linkability (anonymity) setting.

Send data: when sending data, there is a risk that the terms are not displayed in a comprehensive and comprehensible way (note the introduction to this chapter about how crucial a comprehensible presentation is for user's motivation to use secondary functionality). The data transmission might be controlled via a special consent dialogue evoked when data is to be sent. Figure 4-3 shows the "Send data?"-window adapted from the PRIME user interface (Pettersson, 2004b). Figure 4-4 on the other hand shows a service provider's web or WAP page with an example of the "short privacy notice" recently suggested by Article 29 Data Protection Working Party (2004; text adapted from the computer-screen size example in their Appendix 1). Note that in this example it is up to the service provider "Euro Company" to identify themselves. The Working Party argues for the "Acceptance of short notices as legally acceptable within a multi-layered structure that, in its totality, offers compliance." It moreover refers to research stressing not only the need for easily understandable policy notices but also research demonstrating user preference for the layered approach.

Figure 4-3: "Send data?"-window adopted from PRIME

Figure 4-4: Short privacy notice from Article 29 DPWP

Figure 4-5: Pop-up when data is to be sent

Figure 4-4 indicates that the short notices have to be very short to fit snugly into a mobile interface. Possibly, data controller could be left out because this should be obvious from the page framing, but, admittedly, this is a matter of debate. The link to the more complete layer(s) would need to be in a conspicuous place, at least a place that is conspicuous when any *'I agree'* button is visible (which it is not in this figure). An alternative solution would be to allow for smaller pop-ups, which is shown in figure 4-5 and which is in agreement with the working party's suggestion for cases "when individuals are already aware" (ibid.). Yet another alternative could be elaborated around expandable texts within a very short notice; note the discussion in section 4.1 about linking phrases to explanations or to user definition menus (Pettersson, 2004). This will be especially important in cases when fair processing demand more information than only the identity of the data controller and the purpose of the data processing.

In the PRIME solution, the PRIME user-side system may take control of the data transmission and therefore also the information presentation. This may allow for better tailoring. Otherwise the graphical layout of information must be evaluated in all cases and it must be possible for the service provider's system to know what the presentation preferences of the user are.

4.3 Summary

Alerting is a problem if it has to be rather frequent and the environmental circumstances as well as the size of the devices make this problem even bigger for handheld units. Anonymisation provides a reasonable solution to this problem because it makes alerting uncalled for in most cases. Some users may still want to use privacy preference settings and

such settings might benefit from larger displays providing a good overview of different preference details. However, it was noted above that users might use ordinary computers for the privacy preference settings as such settings presumably are done only on rare occasions. A computer could provide a lot of extra help such as digitalised tutorials.

The questionnaires have demonstrated the risk of relying on a *lingua franca* (English) for crucial privacy information on the Internet even for Internet users who are used to visiting English web sites. Privacy policies in machine-readable form constitute a solution because it will be possible to present these in the user's own language, if he has a browser equipped with a suitable interpretator. In the same time one has to be aware that the privacy threats in a networked society are sometimes very intricate. To make ordinary users of varying linguistic and technical skills able to utilise privacy agents will not be merely a user interface problem but will have to be considered in a broader context of how informational self-determinacy are discussed and taught in society.

The difficulties encountered in section 4.2 when adjusting a graphical user interface made for computer screens (the PRIME mock-ups) to mobile phones had to with the difference of size between the mobile's smaller screen and the computer's monitor. The user could, for instance, more easily loose oversight of the program on a smaller screen and there is a risk that the IDM windows will hide other important information. The smaller screen also requires that informational texts be shortened. The standard for information display recently given by Article 29 Data Protection Working Party suggests limiting the demand for immediate display to the very core information plus a link to deeper and more complete layers. This is a reasonable standard for information display. However, for the design of mobile phone screens, every layout, especially of the deeper and more complete layers, must be evaluated. It must be possible for the service provider's system to know what the presentation preferences of the user are, or else the client-side has to be able to take over the structuring of the presentation.

5 Approaches for Mobile Identity Management Systems

This chapter describes approaches for realising the requirements for mobile identity management systems. A complete survey of security systems for identity management will be given in FIDIS study on a "structured overview on prototypes and concepts of identity management systems" (D 3.1) and in the "database on ID laws and identity management systems in the EU" (D 8.3).

Anonymity services are the foundation of identity management, since it enables to user to be anonymous towards his communication partners. Two anonymity mechanisms for mobile users are presented: location addressing and *mCrowds*. Location addressing empowers a mobile user to be anonymous, if his device does not have enough resources for using cryptographic algorithms or if no anonymity infrastructure is available. *mCrowds* establish an anonymity infrastructure without central servers for mobile users in order to minimise the dissemination of personal information on the mobile Internet. A comparison of anonymity mechanisms for *ad hoc* networks shows the advantages and disadvantages of anonymous communication protocols in *ad hoc* networks.

As an example for a mobile identity manager, the research prototype *iManager* is described by its architecture. An example illustrates the use of partial identities in order to protect the user's privacy. In order to link a digital identity with a person, a smart card system called *AXS ID-Card* is later described.

5.1 Freiburg Location addressing as anonymity mechanism

Location addressing is an anonymous mechanism which protects the linkability of the user's interaction with services by the address of his mobile device. The principle of location addressing as an anonymity mechanism is in figure 5-1 demonstrated by the Freiburg *Privacy Diamond* (see section 3.1). Two connections are preserved: the relations between user and device and between action and location. The reason for preserving the relations between action and location is that optimisation based on the current location of the mobile device is possible. The networking infrastructure is able to optimise routing according to where messages associated to the action originate from and go to. In addition, the device can use supporting services in the vicinity of the device, like directory services, because its location does not have to be concealed. Not severing the relations between device and user has the advantage that the users can keep their personal devices. This gives them a trusted environment in which to store personal data.

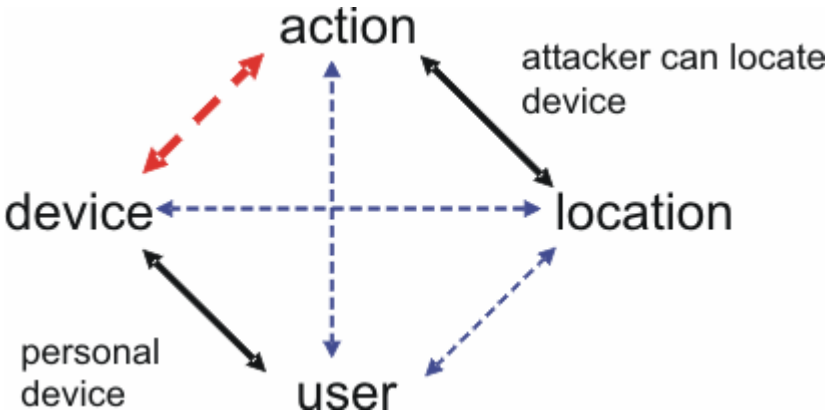


Figure 5-1: Location addressing for protecting the unlinkability of a mobile user

The relationship between user and location are hidden from the attacker by mobility of the user. The user performs actions from different locations which are inconspicuous, i.e. do not allow conclusion of the identity of the user from the location alone. Obscuring the relations between device and location is done in the same manner. To ensure that the attacker is not able to directly link user to action, a tool like an identity manager prevents personally identifying data from being included in the action.

Because only one device can occupy a physical space at a time, it seems natural to use the location of the device as its address. Technical limitations regarding the resolution with which the location can be determined may lead to the situation where two devices have the same address. The same problem can be caused by the fact that actions are not atomic, they may take time during which the device may move. Therefore, an additional part to distinguish between devices that are seemingly at the same location is necessary. This part is chosen randomly (Zugenmaier, 2003).

5.1.1 Architecture of *Freiburg Location Addressing Scheme*

There are two possibilities for implementing location addressing: either as a network layer or sub layer, or within a management plane. Implementation as a separate layer is advantageous because it does not violate the principle of layering within the communication protocol stack. However, it has the major disadvantage that all entities involved in the communication at that layer must implement a location addressing layer, e.g. necessitating changes in routers or similar intermediary devices.

The *Freiburg Location Addressing Scheme (FLASCHE)* implements location addressing as a management plane (Zugenmaier, 2003). Figure 5-2 gives an overview of the architecture of *FLASCHE* on a UNIX based system. This approach has the advantage of keeping the protocol stack mainly unchanged and necessitates alterations only at the mobile device. The examination of the protocols shows that the management plane span transport, network and data link layers. The changes to the HTTP protocol are done with the identity manager of the mobile device, which runs as a proxy at the application layer. The management plane can replace all addresses unique to the device by addresses derived from the location of the device. Addresses unique to the device are used at the network layer, i.e. the IP address and the data link layer, the Ethernet address at the media access layer. Thus, this management plane is able to access the data link and network layers and is able to set the addresses at these layers. The management plane is also be able to associate addresses to TCP connections at the

transport layer and is able to determine when a connection is set up and torn down, in order to determine the lifetime of addresses. The management plane does not access connection information of the application layer, as there are too many different implementations of connection management at this layer. Determination of location is performed outside of the management plane.

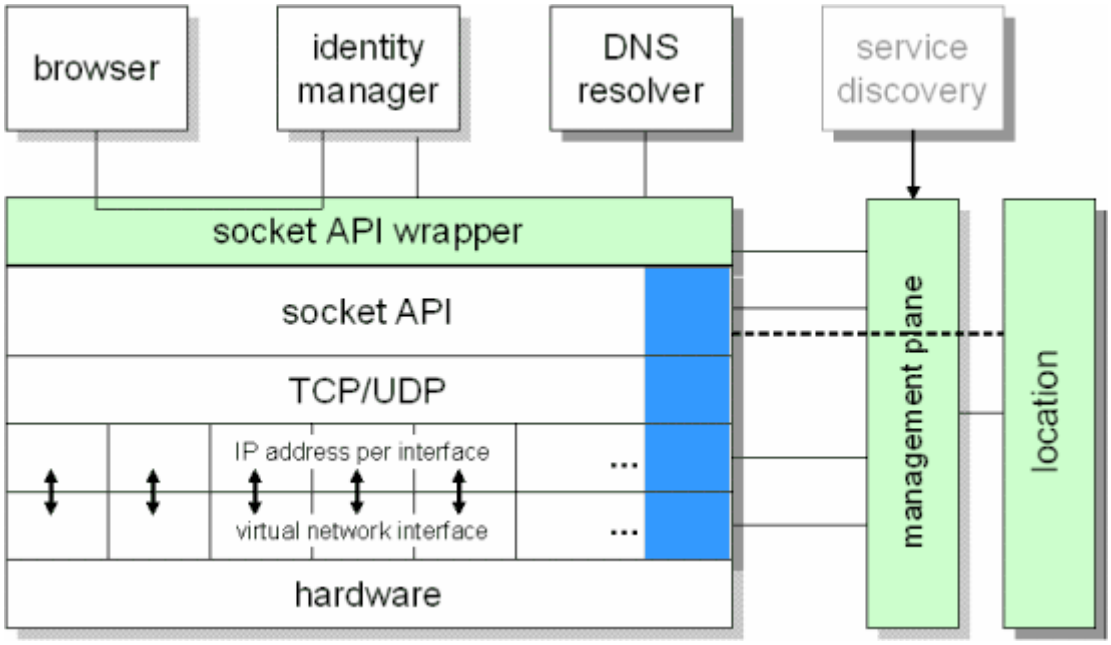


Figure 5-2: Location addressing with browser and identity manager on UNIX based system

Connection supervision is a monitor at the service access point of the transport layer. There all requests for connection set up and connection tear down of the application layer can be seen. The management plane keeps a data structure listing all active connections. Address control derives the device address to be used from the current location. The addresses of the device on the data link and network layers are changed simultaneously. If they were not changed synchronously, the network layer address or the data link layer address would enable linking of actions. A new network layer address could be linked to the network layer address previously used by the same device by correlating the data link layer addresses or vice versa.

5.1.2 Summary

The anonymity mechanism *FLASCHE* exploits a user's mobility to provide anonymity for an action of the mobile user under the condition that the user does not identify himself in the action, the device used to perform that action can not be uniquely identified, and the location of the user and the device does not offer any clues about the identity of the user. The mechanism is resilient to traffic analysis attacks, as they provide information about the location of the device, which by design does not have ot be kept secret. The most serious attack on location addressing is physically observing the location where the action takes place. However, proliferation of the surveillance of public places, coupled with person recognition systems, may make it generally impossible to remain anonymous outside one's

own home. In addition to recognizing the person the surveillance system may also capture the content of the screen of the mobile device.

Proof of concept implementations for all aspects of the described implementation exist, however an efficient implementation of the complete system is not yet realized. Future work also includes anonymous service discovery.

5.2 mCrowds for anonymising WAP surfing

mCrowds (Andersson et al. 2003; Andersson et al. 2004) is a low-latency anonymity technology developed at Karlstad University. The purpose of *mCrowds* is to minimise the dissemination of personal information on the mobile Internet. It does so by enabling anonymous Wireless Application Protocol (WAP) browsing and by minimising the disclosure of personal information when using location-based services (LBS). In cases where the location is measured by the mobile device itself, location based services can be used anonymously if this mode is supported by the LBS provider.

5.2.1 Introduction to Architecture

mCrowds is based on Crowds (Reiter and Rubin, 1997), a system for anonymous web browsing on the traditional Internet. Crowds works by grouping users into a large anonymity set, a so called crowd, which issues requests to web servers on behalf of its members. Crowds is a peer-to-peer technology where each user runs his / her "Mix" in the network (called a jondo) and the communication is routed along virtual paths consisting of many such jondos. A dedicated node called the blender is taking care of membership management. In *mCrowds* the concept of a traditional Crowds system applied in a mobile Internet setting is combined with a personal privacy proxy that acts as a filter tailored to anonymise mobile requests. The figure below illustrates the *mCrowds* system. Note that the crowd itself resides on the wired Internet domain.

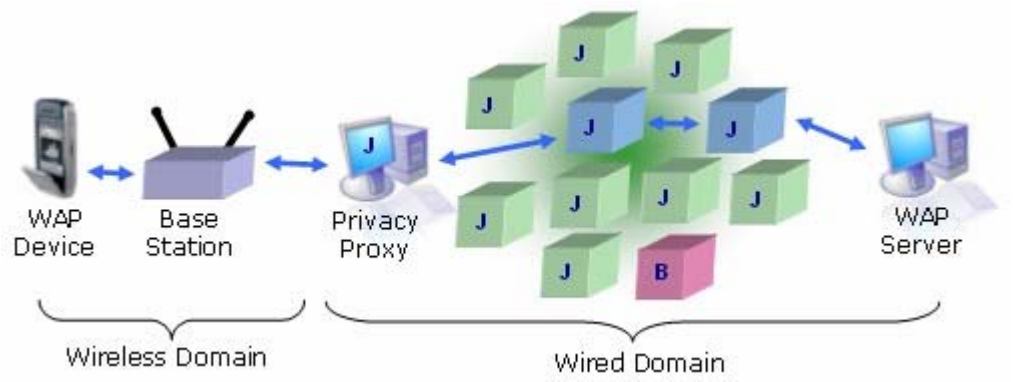


Figure 5-3: *mCrowds* overview

5.2.2 Performance Issues

Performance was one of the primary design goals in the development of *mCrowds*. The traditional Crowds system was chosen to provide a base for *mCrowds*, since Crowds as a base is supposed to offer better performance properties than the more common anonymity technologies based on Mix-nets (Chaum, 1981), such as JAP Web Mixes (JAP, 2003) or Onion Routing (Andersson, 1996). This is because Crowds as a base provides better

scalability properties and further the use of public-key cryptography is minimised. Further performance enhancements have been implemented in the communication protocol of *mCrowds*.

The performance of *mCrowds* has been measured in a performance evaluation that measured the performance overhead introduced by *mCrowds* when browsing anonymously on the mobile Internet (Andersson et al., 2004). To make the conditions realistic, an experimental crowd was simulated where the nodes in the crowds were separated by a relatively large geographical distance. The results of the performance evaluation were encouraging, as the performance overhead was relatively small compared to the total latency. In figure 5-4 below, the total response latency while fetching data from a WAP server is measured. The results are plotted for firstly the case where *mCrowds* is enabled and the path length is four and secondly for the case where *mCrowds* is disabled.

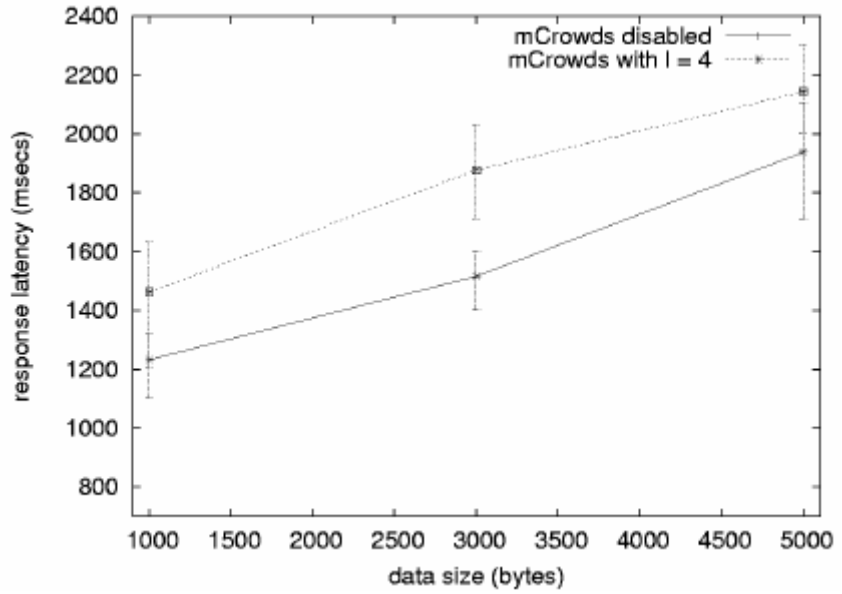


Figure 5-4: Performance evaluation

5.2.3 Conclusions

Mobile Internet introduces new privacy risks and privacy legislation alone is not sufficient to secure informational privacy for users. Thus there is a need to develop privacy-enhancing technologies in addition to privacy legislation. One contribution is *mCrowds*, which is a privacy-enhancing technology that enables anonymous WAP browsing on the mobile Internet.

A number of experiments have been made to evaluate the performance of *mCrowds* in practice, in which the performance overhead generated by *mCrowds* was measured. The subsequent results of this performance evaluation were encouraging as the overhead in performance introduced by *mCrowds* was relatively small compared to the total response latency when fetching WAP pages via the mobile Internet. The results of this performance analysis can serve as a comparison to other approaches for anonymity on the mobile Internet. The area of anonymity and identity management on the mobile Internet is growing fast and such technologies will become more common in the coming years. The contribution in the form of *mCrow*ds can be seen as one of the initial steps.

5.3 Comparison of Anonymous Communication Mechanisms for ad hoc Networks

In this subsection, a comparison of existing peer-to-peer (P2P) anonymous communication mechanisms operating in ad hoc network environments is provided. First, an introduction to P2P anonymous communication mechanisms is presented. Then, requirements are defined according to the ad hoc environmental characteristics in subsection 5.3.2. A comparison of current P2P anonymous mechanisms is given in subsection 5.3.3. Finally, conclusions are provided in subsection 5.3.4.

5.3.1 Anonymous Communication Mechanisms

Anonymity mechanisms are powerful tools that are designed to protect the users' privacy against one or more given adversaries. Anonymous communication mechanisms started to be designed in the beginning of the 1980's, after Chaum's seminal paper "Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms" (Chaum, 1981).

However, until the publication of Crowds (Reiter and Rubin, 1998, 1999; Fischer-Hübner, 2001) in 1997, all anonymous communication mechanisms were based in central servers, also known as mixes, which are responsible for providing anonymity properties to the communication path. The usage of central servers has both disadvantages and advantages.

The advantages include: the mixes identities can be made public through web sites, digital certificates can be easily deployed and used to control authentication between mixes. Anonymous communication mechanisms based on mixes are usually easy to manage as all nodes are well-known (Rennhard and Platter, 2001).

However, the drawbacks are many: mixes can only be deployed on servers with good computing performance and also good network throughput and the number of mixes is limited to few servers and is very small when compared to the potential number of users. Therefore, mixes are potential data traffic bottlenecks and central points of failure. Additionally, intrusions by the law enforcement are easier to deploy, as they can hinder institutions from operating mixes (Rennhard and Platter, 2001).

On the other hand, peer-to-peer (P2P) anonymous communication mechanisms were designed using decentralised and distributed mechanisms based on P2P interactions. The most notorious ones were: Crowds (Reiter and Rubin, 1998, 1999), a proposal by researchers from Bell Labs and AT&T, Tarzan (Freedman and Morris, 2002), from MIT and NYU, MorphMix (Rennhard and Platter, 2001), from the ETHZ (Zurich – Switzerland) and Hordes (Levine and Shields, 2002), a P2P multicast-based proposal from Univ. of Massachusetts and Georgetown University. Other P2P anonymous communication mechanisms are: P5 (Sherwood, Bhattacharjee and Srinivasan, 2002), *mCrowds* (Andersson, Fischer-Hübner and Lundin, 2003), Herbivore (Goel et al, 2003), GNUnet (Bennett and Grothoff, 2003) and Cebolla (Brown, 2002). Recently, other proposals were published in the area, such as AP3 (Mislove et al, 2004) and TAP (Zhu and Hu, 2004). In this document, we focus on the four more notorious mechanisms: Crowds, Tarzan, MorphMix and Hordes.

However, with the advent of *ad hoc* networks, can those existing anonymity mechanisms provide good anonymous properties and good performance at the same time and with a low cost in resources, regarding the limitations of mobile devices? Moreover, are those mechanisms suitable for highly dynamic systems, in which devices are only mobile, but may join and leave the wireless network at anytime? Furthermore, how well do those mechanisms

behave in different network configurations? Can they provide anonymity both in large and small *ad hoc* networks? Answers to these questions can provide an answer to a final question: is it possible to provide anonymity in an *ad hoc* network without relying on the fixed infrastructure of the Internet?

5.3.2 Requirements for Anonymous Communication Mechanisms

In order to answer these questions, some requirements that an anonymity mechanism should follow have to be considered suitable for ad hoc networks. These requirements are:

- Performance: meaning the number of messages needed to establish a secure anonymous tunnel. If the number of messages is too high, then the amount of battery power used to establish a tunnel is also high. Therefore, a good anonymity mechanism should minimise the amount of messages used to establish a secure tunnel. The total number of public key operations needed is also important, as these are expensive operations in terms of computational resources needed.
- Scalability: meaning if a given anonymity mechanism works well under different network topologies and number of nodes. The size of an *ad hoc* network can vary from few nodes only to thousands of nodes. Therefore, a good anonymity protocol should work under different network conditions and topologies, independent of network number of network nodes.
- Security: meaning if the protocol is secure enough against known attacks. The level of anonymity is also included in the quality of security provided by one mechanism. The attacker models proposed in Crowds are used in the comparison (the adversaries). Security against malicious nodes is especially important when dealing with P2P networks.
- Robustness to topology changes. *Ad hoc* networks can be very highly dynamical network environments and an anonymity mechanism has to handle with these changes in the network topology without compromising security and anonymity properties. The agility and flexibility of a mechanism to recover from topology changes are included here. This point is strongly linked with the performance issues, because a good anonymity mechanism shall recover from a topology change with the least number of transmitted messages as possible, in order to save battery power.
- Independence of infrastructure or central servers, such as a Internet based PKI, is a basic characteristic of *ad hoc* networks, because *ad hoc* networks and their services shall still exist even on the absence on a deployed infrastructure.

5.3.3 Comparison of Anonymous Communication Mechanisms

Therefore, we can summarise the comparison of the anonymity mechanisms applied in *ad hoc* networks in the following table. The table contents correspond to a brief summary of the analysis of the mechanisms.

	Crowds	Tarzan	MorphMix	Hordes
Performance	DH between Crowds nodes - in the newest Crowds version	$(L)^2$ messages needed, dummy traffic and (L) public	$6*L+2*\sum(i-1)$ messages,$(4*L)$ public key operations and	DH between Hordes nodes

		key operations	(*L*) DH	
Scalability	Depends on the blender (server) may scale well	May not scale well in large and dynamic networks	Not exactly clear	Different paths from forward and reverse traffic increases scalability
Security	Depends on the probability (p_f) of forwarding messages	Initiator sets the anonymous tunnel path	Collusion detection mechanism	Depends on the number of nodes in each multicast group
Robustness	Tunnel path is rebuild from the broken link	The broken part of the tunnel path is rebuild	The whole tunnel shall be rebuild	Forward path is Crowd similar. reverse path is multicast based
Independent of a deployed infrastructure	No, blender is a directory server	Yes	Apparently yes, but not exactly clear	Membership is controlled by a central server

5.3.4 Conclusions

In spite of the fact that further analysis is still needed to reach a definitive conclusion on the comparison of anonymity mechanisms for *ad hoc* networks, it seems that none of these mechanisms is fully compliant with *ad hoc* network requirements. Therefore, the initial conclusion is that anonymity in *ad hoc* networks cannot be fully achieved with the current proposals and mechanisms for P2P anonymous communication protocols. Therefore, a new anonymous communication mechanism compliant with the requirements of *ad hoc* network environments needs to be designed.

However, the evaluation of future possible mechanisms shall not only consider the aspects regarding the conformance with *ad hoc* networks, but, of course, shall also include an evaluation of the anonymity provided regarding different qualitative and quantitative properties, such as the level of anonymity, the fairness (distribution of the protocol burden among devices), the confidentiality provided, etc. Moreover, different and complementary methods can be used for evaluating some of these parameters. For instance, the level of anonymity evaluation can be obtained using the levels proposed in Hordes in conjunction with the *Freiburg Privacy Diamond* proposal that is based in the attackers' knowledge and has location privacy concerns.

5.4 Anonymity in self-organising Networks – Difficulties and Concepts

In recent years, autonomous, self-organising, wireless multi-hop networks have received increased attention due to their potential applications. In contrast to common communication models, e.g., cellular mobile networks, self-organising multi-hop networks do not rely on any pre-existing infrastructure. Instead, every user-device is a potential intermediate node for forwarding data packets thus becoming part of the network infrastructure. Due to their distributed design these networks become a powerful and reliable tool for establishing a transport infrastructure using equipment already deployed and under operation.

However, ensuring reliable services in self-organising networks raises different problems than in common networks with a centrally managed infrastructure. By large this is due to the fact that for individual nodes, forwarding traffic for others for one is a *losing deal* as it consumes potentially limited resources. On the other hand, each node will need the help of others when trying to send its own packets. Thus, finding a balance and motivating nodes to cooperate in forwarding packets is one of the main problems to be solved in the context of self-organising networks.

In the past few years, a couple of frameworks were presented that encourage collaboration in multi-hop networks. However, all of them have a serious, negative impact on the anonymity of the system, namely keeping the communication relationships unlinkable and ensure the anonymity of the participating nodes. In this chapter we briefly discuss the current approaches and sketch a potential solution.

5.4.1 Related Work

Most models addressing this problem to date are based on the rational assumption of selfish behaviour of participating nodes. That is, a node will engage in the protocol if it is beneficial to do so. Consequently, incentives are used to encourage the nodes to participate, either by rewarding nodes for their efforts of forwarding other nodes' packets (e.g., (Buttyan and Hubaux, 2000; Buttyan and Hubaux, 2003; Jakobsson, Buttyan and Hubaux, 2003; Zhong, Chen and Yang, 2003; Ben Salem, Buttyan, Hubaux and Jakobsson, 2003)) or, by punishing them if a deviation from the protocol is discovered (e.g., (Buchegger and Le Boudec, 2002; Michiardi and Molva, 2002; Marti, Giuli, Lai and Baker, 2000)).

Ad hoc network models. One generally distinguishes between fully self-organising multi-hop networks and hybrid networks. While the former do not rely on the existence of any infrastructure, the latter introduce some operational authority such as, for example, a provider-driven base-station (e.g., (Ying-Dar Jason Lin, 2003; Jakobsson, Buttyan and Hubaux, 2003; Ben Salem, Buttyan, Hubaux and Jakobsson, 2003)). In symmetric hybrid networks both the route to and from the base station are multi-hop. In contrast in asymmetric hybrid networks (e.g., (Jakobsson, Buttyan and Hubaux, 2003)), the routes to any base station are multi-hop while the routes from any base station to any node are single-hop.

Secure Routing protocols. Secure routing protocols such as, for example, (Papadimitratos and Haas, 2002), address security vulnerabilities ranging from DoS attacks, cheating nodes, forging of routing information to impersonation of nodes. Solutions include the use of strong cryptography (e.g., authentication methods, hash chains, threshold cryptography) as well as reputation based methods. Solutions that also address the issues of anonymity and unlinkability include protocols such as (Jiejun Kong, 2003; Jakobsson, Capkun and Hubaux, 2004). While (Jiejun Kong, 2003) uses a public key protected onion (Syverson, Goldschlag and Reed, 1997), Capkun et al. (Jakobsson, Capkun and Hubaux, 2004) propose a solution for hybrid networks in which the operator not only has access to location and identity of registered nodes but also shares a secret key with each individual node.

Incentive mechanisms. Mechanisms to encourage collaboration can be positive (reward) or negative (punishment) in nature. The latter approach is, for example, taken in reputation systems like CONFIDANT (Buchegger and Le Boudec, 2002), CORE (Michiardi and Molva, 2002) and the watchdog/pathrater approach by Marti et al. (Marti, Giuli, Lai and Baker, 2000). They mainly consist of sophisticated observation and reporting mechanisms combined with a clear punishment strategy. Rewarding systems like (Buttyan and Hubaux, 2000;

Buttyan and Hubaux, 2003; Jakobsson, Buttyan and Hubaux, 2003; Zhong, Chen and Yang, 2003; Ben Salem, Buttyan, Hubaux and Jakobsson, 2003), on the other hand, employ some payment or crediting system in order to charge and reward participants: one participant (in most cases the originator or the destination) is charged for services and all intermediate nodes along the route are paid for their forwarding efforts. In hybrid networks, the base station can monitor packets, enforce the rewarding policy and detect attacks (Ben Salem, Buttyan, Hubaux and Jakobsson, 2003; Jakobsson, Buttyan and Hubaux, 2003). In self-organising multi-hop networks, on the other hand, rewards can, for example, be redeemed through a clearing authority (Zhong, Chen and Yang, 2003). An alternative approach, is the local broadcast technique (Buttyan and Hubaux, 2000). This technique links the actual forwarding of packets with remuneration. The information a node needs for getting remunerated is included in the packet which is sent by the subsequent hop. Receiving the broadcast from the next hop forwarding the original package confirms that the claiming node forwarded the package and that it was received by the next hop. The technique relies on the assumption that radio links are symmetric.

Most incentive schemes proposed to date require some sort of trust. Trust is established, for example, by means of a public key infrastructure (e.g., (Zhong, Chen and Yang, 2003)) or through the use of tamper-resistant hardware—which can be viewed as a distributed trusted third party (e.g., (Buttyan and Hubaux, 2000; Buttyan and Hubaux, 2003; Jakobsson, Buttyan and Hubaux, 2003)).

5.4.2 An untraceable incentive scheme

The main problem which is not yet addressed by common solutions is how to provide incentive mechanisms for multi-hop networks which not only encourage collaboration between nodes but at the same time keep communication relationships unlinkable and ensure the anonymity of participating nodes. In single-hop wireless networks, e.g., base-station-oriented cellular networks, a subscriber can obtain a sufficient level of privacy by deactivating his device while not sending or receiving data. In contrast, in multi-hop networks the user is required to keep his device activated at all times in order to maintain a viable networking infrastructure for everyone.

In the following, we sketch a protocol that not only meets the increasing need of (location-) privacy but also provides an efficient incentive mechanism for forwarding packets in a multi-hop wireless network (Alkassar and Wetzel, 2004).

Incentive Mechanism. The incentive mechanism is based on electronic coins as a system-wide currency. Each node may withdraw coins from and clear coins with a so-called clearing service[4]. The system allows for coins of different but fixed denominations. For each intermediate node (on the route from the source to the destination) the source node will withdraw one coin of sufficient denomination from the clearing service. The denomination of a coin directly corresponds to the maximum number of data packets to be transmitted during a session. That is, in order to have n intermediate nodes each forward p data packets (of fixed size), the source node must withdraw n single coins of denomination $p \leq d$ from the clearing service. Coins are valid for one particular session only, used portions of a coin cannot be used up in subsequent sessions. A node is charged upon withdrawing coins and rewarded when

4 It is also the clearing service which handles the exchange of electronic coins and real money. The system can be generalized using multiple (possibly hierarchically organized) clearing services.

presenting received coins. Rewards are given only in the amount corresponding to the actual number of forwarded packets.

A source node may claim refund for the difference between the denomination of the coin (used to pay an intermediate node for its efforts during a particular session) and the amount corresponding to the packets for which a reward was claimed.[5] For simplicity we assume that every node can regularly establish a direct, i.e., single-hop link to the clearing service. In order to assure unlinkability, the refund is to be handled by a separate trusted third party.

Security model. The system is considered to be secure if the incentive mechanism is fair and messages, respectively participants are anonymous and unlinkable. The incentive mechanism is fair if no node can gain any (monetary) advantage by cheating, i.e., deviating from the protocol. With respect to cheating one generally distinguishes (see for example (Ben Salem, Buttyan, Hubaux and Jakobsson, 2003)) between the *refusal to pay* and a *false reward claim*. The latter is a node trying to claim monetary reward for packet forwarding he never performed. The refusal to pay is characterised by a node refusing to pay for the forwarding services performed by intermediate nodes. *Free-riding* is a special case of refusing to pay in that collaborating nodes are trying to misuse the protocol in order to avoid charges (e.g., by interleaving sessions, using side-channels).

The Scheme. Skipping the details of the building blocks, we can now describe our construction for an untraceable coin-based incentive scheme. We discuss each one of the stages *set-up*, *withdrawal*, *packet delivery* and *rewarding* separately. A more sophisticated, alternative protocol that allows for more flexibility in terms of the payload to be transmitted can be found in (Alkassar and Wetzel, 2004).

Set-up. The clearing service and the nodes are set up as in Brands' payment system (Brands, 1993). That is, the clearing service generates different h_d's for different denominations D_d and publishes them in a non-repudiatable way.

Withdrawal: A source node *S* intending to send a certain number of payload packets with the help of *n* intermediate nodes is required to withdraw at least *n* coins of sufficient denomination in order to pay for the service. The withdrawal is done as described in Brands' payment protocol (Brands, 1993).

Packet delivery. In order for a source node *S* to send a number of data packets to destination *D*, the source node *S* will first use a corresponding route discovery protocol to determine route R^D_S to destination node *D*. Source node *S* may receive several answers to its route request corresponding to alternative routes to reach the destination *D*. The source node will select one route (e.g., one with the least number of hops in order to minimise costs). Let $||_{i=1,...,n}\ (k_i,r_i)$ be the route description for the selected route and let $N_1,...,N_n$ be the intermediate nodes on this route.

Using the selected route R^D_S, the transmission of the payload packets is organised in two steps: The initialisation step in which one coin is sent to each one of the intermediate nodes and the packet delivery step itself, in which the data is sent. In order to simplify matters, we

5 Every coin is valid for some fixed, limited time only. Refunds may be claimed after a coin has expired. Since the internal clock of one node may deviate from the internal clock of other nodes in the ad hoc network, nodes should accept coins only which have enough time left until expiry.

will first focus on the structure of the messages sent during payload delivery. Afterwards, we will discuss the initialisation phase in detail.

Payload message structure. Let $p \leq d$ be the number of packets that S intends to send during this particular session. We write msg^i_j for the i-th packet (i=1,...,p) sent by the j-1st node to the jth node on the route from S to D. The system is designed such that the last message (sent from node N_n to D) is of form

$$msg^i_D = enc_D(payload)$$

and for nodes N_j (j=1,...,n) of form

$$msg^i_j = enc_{kj}(msg^i_{j+1}).$$

Initialisation phase. At first, the source node computes so-called authenticators $A^p_j = ||_{i=1,...p} a^i_j$ as they will later on be seen by the respective intermediate nodes N_j ($1 \leq j \leq n$). The individual components a^i_j are defined as

$$a^i_j = hash_0(hash_1(msg^i_{j+1}))$$

(i corresponds to the ith packet with $1 \leq i \leq p$) using two one-way hash functions $hash_0$ and $hash_1$6. Now S can send a coin $coin'_j$ to each intermediate node N_j with $coin'_j = (A,B,\sigma,r_1,r_2)$. In order to ensure that the coin is bound to both the respective node as well as the corresponding authenticator A^p_j, we need to extend payment step in Brands' scheme by adding the authenticator A^p_j to the hashed challenge, thus obtaining $C = \mathcal{H}(A,B,n,A^p_j)$. The actual initialisation messages msg^0_j are determined as

$$msg^0_j = enc^e_{kj}(coin'_j, A^p_j, msg^0_{j+1}) \text{ and}$$

$$msg^0_n = enc^e_{kN}(coin'_j, A^p_N)$$

with j=1,...,n-1. Upon receiving msg^0_j, node N_j verifies the signature within the coin (as in Brands' payment step).

Sending of data packets. After completing the initialisation, the source S can send off the data packets. The intermediate node N_j, receiving msg^i_j (corresponding to data packet $1 \leq i \leq p$), will decrypt and authenticate the message using its private key k_j. If decryption was successful (i.e., did not return $\perp$), node N_j may forward the decryption result $msg^i_{j+1} = dec(msg^i_j)$ to the next intermediate node N_{j+1} on the route to destination D.

Rewarding. In order to ensure that only those coins can be cleared by intermediate nodes for which the respective packets have been forwarded by the node, the nodes must justify their claims by providing additional information. According to our model, messages are broadcasted and network links are assumed to be symmetrical. Hence, node N_j will also receive msg^i_{j+2}, the message sent from hop N_{j+1} to N_{j+2}. The sending of this message, however, can not occur unless node N_j had complied with the protocol forwarding msg^i_{j+1} to node N_{j+1}

6As we will see later, the first hash pre-image enables the node to authenticate the incoming message, while the pre-image of the hash pre-image will later on be used as a proof for correct forwarding of a message.

which in turn decrypted the message and sent on msg^i_{j+2}. Thus, node N_j will keep $x^i_j=\mathcal{H}_1(msg^i_{j+2})$ as authenticator. Together with $coin'_j$ and the preimage x^i_j of a^i_j, N_j can prove its claims.

Except for the rewarding stage, the anonymity and unlinkability follows directly from the property of semantic security of the encryption algorithm and that every combination (k_j,N_j) is used only once.

Anonymity and unlinkability during the rewarding stage is guaranteed because of the anonymity and unlinkability property in Brands' payment scheme: Linking two nodes in the rewarding stage would enable linking of two coins which in turn would break the underlying payment scheme. This is due to the fact that the coins are only pair wise known (onion encryptions) and in the basic protocol the authenticators have no relationship to other nodes. In the alternate protocol, the authenticators are linked to other nodes authenticators. However, for anybody else than the intermediate node and the source node, the authenticators are indistinguishable from random data.

5.4.3 Outlook

The problem of encouraging cooperation in multi-hop networks, while keeping the participating nodes anonymous is still a challenging task.

So far, we proposed an incentive scheme, based on a common anonymous, coin-based payment scheme. In terms of future work, we intend to incorporate an efficient error handling and acknowledgements into the protocol making reliable packet delivery more efficient. Finally, we will explore how to realize an anonymous routing protocol that prevents free-riding, which still seems to be an open problem.

5.5 iManager – Identity Manager for Partial Identities of Mobile Users

An identity manager called *iManager* for mobile users is developed at the University of Freiburg, Germany. *iManager* enables a mobile user to communicate securely, to manage his partial identities and consequently to protects his privacy. It fulfils the requirements I.a, I.b, II.b, III.b, IV, V, IX.c and IX.d of section 2.1. This identity manager is a client side identity manager, which means that the partial identities are managed solely by the user and not by a third party. The identity manager is part of the mobile device of the user which is considered to be trustworthy. The use of *iManager* is described by an exemplary scenario: buying and inspection an electronic railway ticket (Gerd tom Markotten, Wohlgemuth and Müller, 2003). In this scenario, the *iManager* has interfaces in order to use the applications of the mobile devices: electronic ticket application, a digital wallet and a web browser. The following section describes the architecture of *iManager* applied to this scenario.

5.5.1 Architecture of the *iManager*

The *iManager* is the central security tool of a mobile device. It offers interfaces to the user, to the security mechanisms and to the applications of a mobile device. The access to personal data and to cryptographic keys is exclusively possible by using the identity manager. An application's request to these data will be checked by the identity manager to see whether the user has given consent to the publication of this personal data. The architecture of the

iManager and its interfaces is shown in the figure 5-5. Based on a *security platform* with the necessary security mechanisms in order to protect the communication, the personal data and the privacy of the user, the components *identity configuration*, *identity negotiation* and *confirmation of action* are responsible for managing partial identities (Jendricke and Gerd tom Markotten, 2001).

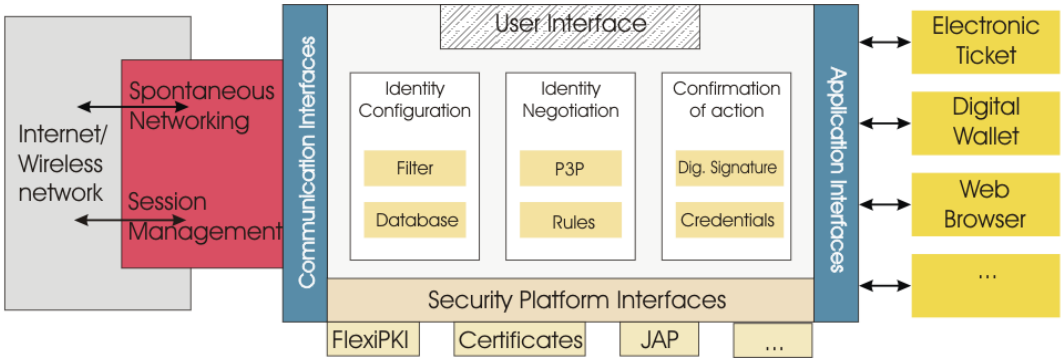


Figure 5-5: Architecture of the *iManager*

The *user interface* has to be comprehensible for security laymen, since they are not able to verify and assess the security mechanisms of the iManager and therefore a misuse of them leads to a compromise of the security and privacy of the user. The possibilities of a misuse have to be reduced (Gerd tom Markotten, 2004). The acceptance of the security tool depends on its user interface as well. In order to facilitate the use of a security tool, the protection goals of multilateral security (Rannenberg, Pfitzmann and Müller, 1997) have been classified in user and system controlled protection goals by analysing their interdependency (Jendricke and Gerd tom Markotten, 2000). This leads to a reduction of the user interface's complexity. The user controlled protection goals *anonymity* and *accountability* are configured by partial identities and their choice in a situation. The integration of the *iManager* in the user interface of the mobile device is shown in the figure 5-6. At any time, the user is able to check his identity.

Figure 5-6: Integration of the iManager in the user interface of the mobile device

The *identity configuration* enables a user to choose and create a partial identity with respect to the current situation. A situation is defined by a communication partner, the current service and the current partial identity (Jendricke, Kreutzer and Zugenmaier, 2002). Since the anonymity level cannot increase subsequently (Wolf and Pfitzmann, 2000), any partial identity can not be chosen. If the user wants to change the current partial identity, the *iManager* checks if the desired anonymity level could be reached with the intended change. This component is realised functionality to edit partial identities and to store them in a secure database on the mobile device and to recognise the current situation. The secure database stores partial identities and user's security, his privacy policies and rules for the security tools. A filter checks the data flow of the mobile device for personal data. By this means, it is possible to fill a web form according to P3P with respect to a suitable partial identity and user's permission.

An *identity negotiation* is necessary, if a service needs more data from the user than he wants to publish in this situation. This conflict can be solved with a negotiation between this service and the user. A restricted automatic negotiation is possible by the implementation of P3P and consequently the comparison from the service's and user's security and privacy policy. In case of a conflict, *iManager* informs the user of this conflict and proposes solutions like a suitable partial identity for solving it. For example, in the scenario where a user wants to buy an electronic railway tickets and wants to get some premium points. For the premium points, the virtual ticket automaton requests some personal data of the user. A conflict occurs since the user acts with his partial identity *anonymous*. The *iManager* proposes to use the partial identity *traveller* for solving this conflict. Figure 5-7 shows this case.

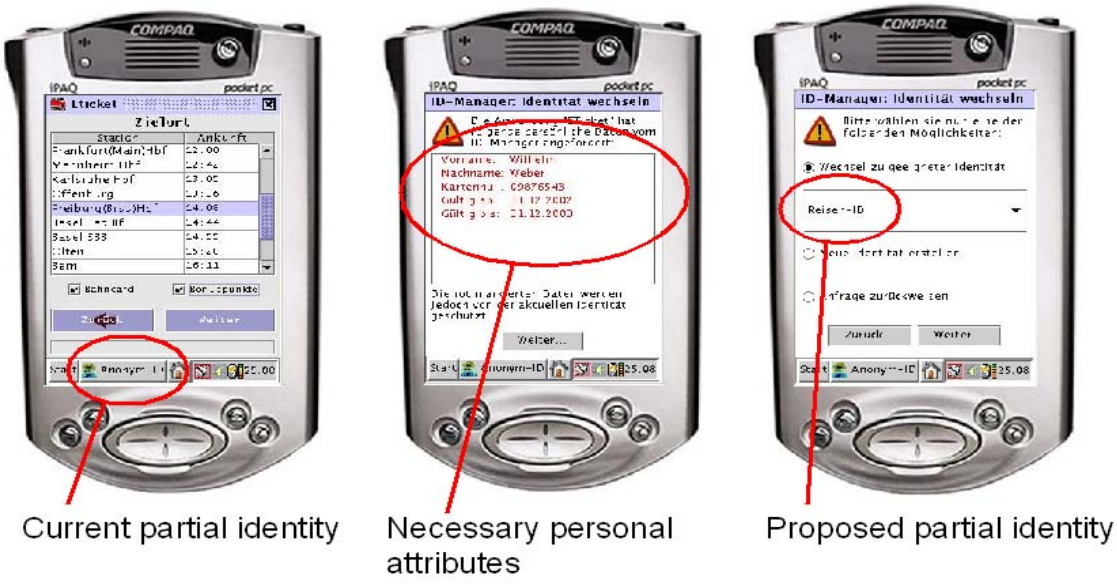


Figure 5-7: Identity negotiation

The user decides his accountability and the accountability of his communication partner for each partial identity. The component *confirmation of action* realise the accountability of the user by a digital signature tool. It is used whenever a digital signature is required, e.g. for self-signing personal data. Since the user declares explicitly his intent, he signs with his handwritten signature and authorises the digital signature tool to sign the corresponding credential. The digital signature key is chosen by choosing the suitable partial identity. By this means, the technical functions of the key management will be shown in a more comprehensible manner (Gerd tom Markotten, Jendricke and Müller, 2001).

The *security platform* consists of interfaces to cryptographic primitives, anonymity services, to a session management, a secure database and to security services. Anonymity services are the foundation of identity management, since it enables to user to be anonymous towards his communication partners. The anonymity service JAP (Berthold, Federrath and Köhntopp, 2000) is used for IP networks. For spontaneous networking, a library from the University of Rostock, Germany, (Sedov, Haase, Cap and Timmermann, 2001) is used. The cryptographic primitives for encryption and digital signatures are realised by the library FlexiPKI (Buchmann, Ruppert and Tak, 1999).

5.5.2 Summary

The *iManager* of the University of Freiburg, Germany, shows that it is feasible to realise privacy and security interests of a mobile user depending on the situation by managing and appearing with different partial identities. It is further developed in order to support business processes in which services are acting on behalf of the user towards personalised services. In this kind of business processes, the user has to confidentially delegate some of his authorisations or partial identities to strange service providers while acting under a pseudonym.

5.6 AXS ID-Card

The *AXS-Authentication Platform*™ comprises technologies for the remote authentication of persons at Internet portals or at physical gates. The platform has an open and modular architecture that allows an implementation of the *AXS-authentication* in any web-based Extranet Access Management System (EAM) using standard Web technologies. The *AXS authentication* can also be implemented within any other Identity Management System (IMS) or existing authentication scheme. The platform includes tools and mechanisms (Müller, Jacomet and Cattin, 2002) that:

- enable secure, mobile, ergonomic and privacy protecting authentication at physical gates or logical portals,,
- enable the use of federated identities over multiple networks and operators (requirement VI and VII of section 2.1),
- enable digital signature-codes on transaction documents proofing authenticity and integrity of an e-business transaction for both sides (requirement VIII of section 2.1),
- enable the storage of key seeds and the use of pseudonyms for a secure and privacy guaranteed access to databases with sensible data (requirement III and IV of section 2.1) and
- allow immediate and user-friendly roll-out, deployment and management of the identity credentials as no local HW or SW installation is needed, an Internet connection and a browser is sufficient (requirement Id, X of section 2.1)

5.6.1 How the *AXS-ID-Card* works

The key element is a set of functional components that are integrated in a personal token, in the shape of a credit card – *AXS-ID-Card* – that people can carry in their wallet or that can be attached to other personal belongings like a PDA or a Handy. It enables the owner to prove his identity anytime and anywhere at physical gates and inter- or intranet portals through an optical and/or RFID interface. The device also allows him to generate a digital signature code or to get remote access to an encrypted database with personal data, e.g. for E-health applications.

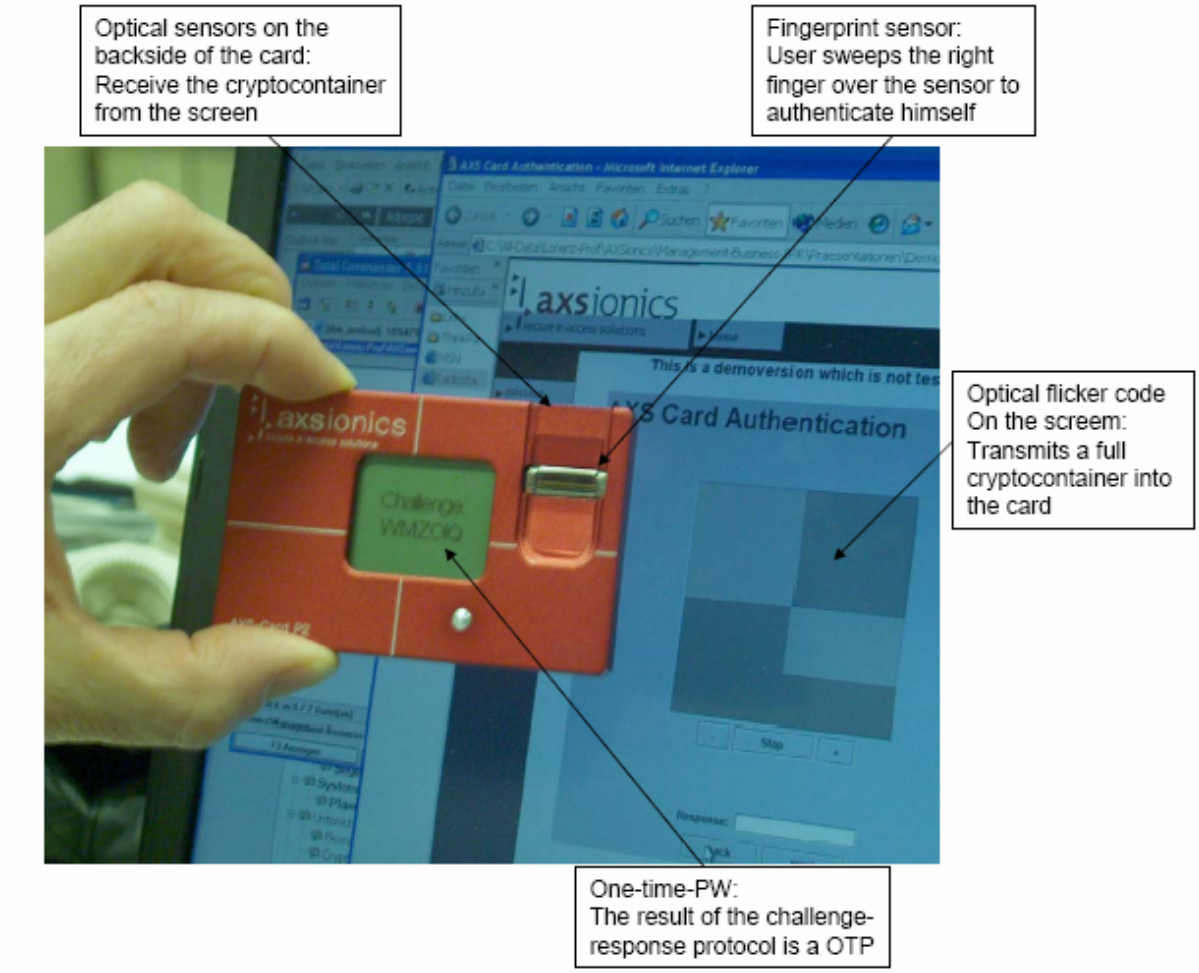


Figure 5-8: The *AXS-ID-Card*

The *AXS-ID-Card* works with a simple user interaction protocol:

a) The user requests login to a closed site that is protected by the *AXS-authentication scheme*. The site sends a message including a crypto-container with the one time password directly on the screen in form of a flickering code.

b) The user starts the card to authenticate him by sweeping a finger over the sensor. On power up the card displays information that defines the specific finger to sweep for the actual authentication. Only the authorised user can link the displayed information with the right finger (user secret)

c) The card verifies the user's identity matching the acquired fingerprint pattern with the stored template of the requested fingerprint.

d) The user reads the message with the encrypted challenge from the screen holding the card over the flickering code. The card links the received crypto-container with the corresponding key in the card that has been allocated for the specific site to decrypt the challenge.

e) The card displays the decrypted OTP (One Time Password) on the card display;

f) The user returns the OTP to the authentication server of the protected site to get access.

This authentication protocol can be used independently by different authentication servers. At initialisation of the *AXS-ID-Card* a set of yet inactive keys are stored inside the card. The physical card represents thus a container for an in principle unlimited number of independent identity credentials that may be used for authentication in different networks. At the time of enrolment the user gets the corresponding certificates for the stored identity credentials. He may deposit these certificates at a certification authority of his choice for later distribution or he may deliver certificates one by one to the authentication servers of the networks he wants to be registered as authorised user. This scheme allows him to realise Single Sign On (SSO) and/or federated identities without compromise on privacy or availability. The network operator that receives a certificate from a user who wants to register for the network services must only trust that the provider of the card runs a proper enrolment process.

5.6.2 Functionality of the *AXS-authentication scheme*

The *AXS-Authentication Platform*™ builds up on a proprietary technology with open interfaces respecting the upcoming standards in the field (WSS, SAML of OASIS). The *AXS-ID-Card* is an interface device which identifies, on one side, the authorised user with a two or three factor authentication. On the other side, it connects to digital networks through optical, acoustical, electronic or RFID-NFC (Radio Frequency Identification- Near Field Communication) interfaces. The optical (and optionally the acoustical) interface provides a one way input channel. The return channel goes via an LCD display to the user and then via keyboard back to the server. The implemented functions are:

- Online authentication of user

  Verification of a user identity (authentication) with a challenge response protocol that provides a unique one-time PIN- or pass-code that can be submitted from any terminal in the world

- Server identification, prevention of phishing attacks

  Verification of the server identity through the user with a simple optional add-on to the basic protocol; prevention of phishing or other forms of man-in-the-middle attacks with a simple modification of the basic protocol delivering some additional information to the user enclosed in the crypto-container that is not accessible to the man-in-the-middle attacker.

- Provable transaction signature

  Digital transaction code related to a document proofing mutual agreement on a transaction between provider (server) and user (card holder)

- Privacy secured database access

  Storage and retrieval of a key giving access to encrypted private data on a centralised database

- Privacy protecting roaming between service networks

  Different unlinked pseudonyms for the authorised user on the same card available (actual up to 15 virtual cards enclosed in one physical card, may be extended to much higher numbers), user determined disclosure of identity information

- Tracking, licence control etc.

  Several other functions can be implemented on the system without altering the basic technology, e.g. the link of a SW-licence to the user, user controlled passive tracking of the card inside a building with the RFID tag (the default setting for the tag is mute).

5.6.3 Fulfilment of requirements for mobile identity management

The *AXS-ID-Card* is an autonomous mobile authentication token (see section 2.8) that fulfils the requirements of section 2.1:

- Identity Administration (requirement I): The card stores an arbitrary amount of independent unlinked digital identities which can be used with pseudonyms and different profiles. Through the optical transmission channel, a server can also send an application specific credential directly into the card that the user can present in an appropriate situation (e.g. digital ticket in form of a 2D-barcode on the card display)
- Notice (requirement II): For each digital identity the card logs the most recent transaction history
- Control (requirement III): The user has full control on all interfaces including the RFID communication channel, which can be switched off whenever the user wants to avoid the traceability of the card. The user can prove to a third party that he has been authenticated by his *AXS-ID-Card* without disclosing any relevant identity information. A trusted anonymity within the set of users that have an *AXS-ID-Card* can be achieved through this mechanism.
- Security (requirement IV): The *AXS-ID-Card* provides authentication and transaction certification protocols that are secure and integer at the level of today's strong asymmetric cryptography. The availability is achieved with the communication channel over the computer screen to deliver a crypto container into the card and the on card display for the user to be returned over the keyboard.
- Privacy (requirement V): The user has always the full control over the *AXS-ID-Card* communication. No personal identity information is ever disclosed by the card. The certificates that are linked with the independent internal identity credentials (keys on card) contain no personal information. The only deliver the proof that a specific credential will represent an identity that is linked with one *AXS-ID-Card*. The user then is free to deliver additional personal information to the operator.
- Interoperability (requirement VI): The *AXS-ID-Card* is a container for multiple digital identity credentials. SSO and federated identities are realised directly on the card
- Trustworthiness (requirement VII): The editing certification authority provides each card with a number of digital identity certificates. The card hardware will be certified for its tamper resistance. The card allows mutual authentication between server and user. All implementations of the mechanisms follow open standards for Web services (W3C and OASIS standards).
- Liability (requirement VIII): There are protocols that allow the generation of digital signatures and non-repudiation transaction codes. Inside the card there is a limited transaction log that may be read out with the explicit consent of the user.

- Usability (requirement IX): The user interface of the *AXS-ID-Card* is reduced to a few key functions. Most of the security functions are hidden from the user. The handling of all credentials are done directly in the card, there is no exchange of identity information between different operators. This reduces the complexity of a federated identity management system tremendously.
- Affordability (requirement X): The *AXS-ID-Card* uses no licensed software. Its cost is in the same range as other authentication tokens (SecureID, Vasco cards etc). As far as possible open source building blocks arte used for the *AXS-platform* and its integration.

5.6.4 Summary

The *AXS-authentication scheme* is a novel approach to generate a tide link between a physical person and its digital identity. The introduction of a dedicated personal device that serves as a portable electronic identity credential manager in form of a thick credit card allows accomplishing requirements for privacy enhancement, security and availability without compromise. The scheme is flexible to adapt for future needs like large scale federation of identity management or the integration of extranet access management, intranet login and physical access control in one IMS. The risk of identity theft at large scale is reduced as there are no high risk centralised repositories with personal identity information. It also eases the response to future social engineering attacks as an attack has to be executed card by card and thus can not be automated. The *AXS scheme* hereby shows how biometrics can be included in the authentication process without a high risk for the privacy of the users.

6 Conclusion and Outlook

6.1 Conclusion

Mobile Identity Management is in its infancy. For example, GSM networks provide with the management of SIM identities a kind of mobile identity management, but they do not realise all requirements for mobile identity management as they are summarised in this study. Unlike the static identity already implemented in current mobile networks, dynamic aspects, like the user's position or the temporal context, increasingly gain importance for new kinds of mobile applications. Some needs for mobile identity management have been presented by scenarios for authentication of mobile users and billing / payment purposes. Privacy and the protection against identity theft are important decision criteria for services which make use of a mobile identity. It has been shown that cryptographic protocols are not sufficient against identity theft and that tokens which stores biometric data of its user and has its own biometric sensor are actually best suited to link a physical with its digital identity.

Two new privacy threats for mobile users in contrast to stationary users have been considered in this study. These threats for mobile users are their location information and their personal preferences for the configuration of their mobile device's user interface. With the help of the Freiburg Privacy Diamond, anonymity mechanisms can be analysed, since it takes the mobility of a user with one mobile device into account. The discussion and comparison of anonymity mechanisms for *ad hoc* networks with MobileIP have shown that no current proposal for anonymity in *ad hoc* networks is suitable. One approach is to develop new anonymity mechanisms. Another approach is the use of an anonymous incentive mechanism in order to establish an infrastructure in an *ad hoc* network and therefore to enable the use of current anonymity mechanisms, e.g. *mCrowds*.

In addition to privacy, usability of mobile identity management systems is important for the success of mobile identity management, too. Usability influences the correctness of security mechanisms. Since being secure is not a primary goal of a user and user do not want to learn security mechanisms, mobile identity management has to be comprehensible for security laymen. This study has focussed on the design of mobile identity management systems. Vocabulary tests have shown that the privacy terminology is too technical to be readily intelligible for lay English users. In addition, new layouts for configuring the privacy preferences have to be developed, since the small display of mobile devices.

But there exists approaches for mobile identity management. Besides the anonymity mechanisms *Freiburg Location Addressing Scheme* and *mCrowds*, the identity manager *iManager* empowers a mobile user with his mobile device to manage his identity and to protect his privacy by controlling the disclosure of his personal attributes. Linking a physical identity with its corresponding virtual identity is possible by the *AXS ID-Card* system.

6.2 Outlook

This study (D3.3) will be extended in WP11 (D11.1), by gathering additional information on the state of the art of mobile concepts, such as the SIM, USIM or WIM (WAP Identity Module) as well as other identity standards from mobility related organisations (e.g. the Open

Mobile Alliance, ETSI, etc.). The resulting issues will be extended from wireless and mobile to satellite communication and location based services (LBS).

The objectives of work package 11 (WP11), "Mobility and Identity", for the FIDIS Network of Excellence are the identification, the description and the application of the concepts and elements in the fields of mobility and identity. The subject of research and discussion will be the identification and description of the term 'mobile identity'.

Another major task of WP11 will be the economic evaluation of such systems and their influences on our everyday life. While technical aspects of mobility and identity are researched in depth, economic aspects seem to play a minor role in this domain. Nevertheless, from an economic point of view, these questions are important for decision making in a commercial set-up.

The assessment of new business models, such as they were presented in chapter 2.3 and mobile services will be the key factors to be analysed in this context. Furthermore, the market acceptance of the used technologies and other effects, such as legal, socio-cultural, and so on, will be taken into consideration. Especially for advanced data services, such as location based services (LBS), new identity management concepts are needed in order to enable secure communication and what information is need to provide a service.

Although being quite innovative, some of these services and products using mobile identity management systems disappeared, due to the fact that they were not profitable or they did not succeed in getting into the market. Possible reasons might be the lack of integration of the system, its usability, or the willingness of the customers to use an identity management solution. Consequently, looking from the standpoint of a for-profit organisation, it is crucial to ask for the profitability of mobile identity management systems and their usage. Especially looking at the variety of emerging and constantly changing technologies, it is difficult to find a generic model – "Technology changes; economic laws do not" (Shapiro and Varian, 1999).

Personalised services seem to improve the quality of people's lives by acknowledging their needs, requirements and preferences and thus acting in some way on their behalf. In order to support such business processes in which services are acting on behalf of the user, mobile users have to be supported to confidentially delegate some of his authorisations or partial identities to strange service providers while protecting their privacy by usable mobile identity management. Furthermore, today's anonymity mechanisms do not fully meet the requirements for mobile *ad hoc* networks. One approach is to develop an anonymous overlay network suited for mobile *ad hoc* networks.

Some of the arising questions to be answered in the context of the evaluation of the profitability of mobile identity management systems, which need to be addressed, are:

- In which temporal context am I conducting an evaluation (ex ante or ex post)?
- What is the composition of the market I am looking at (e.g. public or private customers)?
- Who are the key players, which participate in the observed market (e.g. mobile operators or, customers, governments) and what are their goals?
- What are the driving factors for the evaluation of the market for mobility and identity and how do they affect each other (e.g. technology acceptance, usability, market penetration, market competition, market share, etc.)?

- How to model the environment and the interaction of the key-players among each other?

Furthermore, the complex nature of such markets and their parameters makes it difficult to come up with a generalised approach for an economic evaluation. Nevertheless, by using a combination of different methods, such as simulation approaches or economic theories, one can analyse the possible direction of the future development of such technologies and their diffusion into the market.

7 Glossary

- **aMAD – autonomous Mobile Authentication Device**

  It describes a token that authenticates its user without additional interactions with any external equipment through on board authentication interfaces (biometrics, keyboard for a secret). The device then delivers digital signals for the identity of the authenticated person over available channels (display with a one time password, RFID, smart card interface etc.)

- **ATM – Automated Teller Machine**

  Automated teller machines (ATMs) allow customers to carry out bank transactions without the assistance of a teller.

- **CR protocol – Challenge-Response protocol**

  A challenge response protocol is used to authenticate ad-hoc a person or a machine. In a CR protocol the authenticating instance generates a random string (challenge) and sends it to the instance that has to be authenticated in a way that only the receiver who possesses the right identity credential can recover and interpret it. The receiver sends information back to the sender (response) that proofs that he was able to receive and correctly interpret the challenge. Typically the a CR-protocol is based on a PKI (FIPS Pub 196), but also other forms like zero-knowledge protocols fall (e.g. Fiat-Shamir protocol) under this category.

- **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.

  - ***Idem identity:*** A concept that links a ”token“ from the digital / syntactical world to an object in the real / semantic world, which is provided by the SIM/GSM-infrastructure.
  - ***Ipse identity:*** A set of properties and attributes describing the situation and context of the mobile subscriber.

- **DDS – Direct Digital Synthesizer**

  Direct digital synthesizer (DDS) is a fine resolution digital frequency synthesis technology that uses a numerically controlled oscillator (NCO) to program the output frequency to the chosen value.

- **DNS – Domain Name System**

  The Domain Name System or DNS is a system that stores information about host names and domain names in a kind of distributed database on networks, such as the Internet. Most importantly, it provides an IP address for each host name, and lists the mail exchange servers accepting e-mail for each domain (Wikipedia, 2005).

- **DoS Attack – Denial of Service Attack**

  A Denial of Service attack (DoS) is an electronic attack whose purpose is to prohibit an opponent the use of a dedicated part of or the entire system.

- **D/A converter**

  A digital-to-analog converter is a device used to convert digital signals to analog signals.

- **EAM – Extranet Access Management**

  An extranet is an extension of a corporate intranet using World Wide Web (WWW) technology to facilitate communication with the corporation's suppliers and customers outside the secured company perimeter. An extranet allows customers and suppliers to gain limited but secure access to a company's intranet in order to enhance the speed and efficiency of their business relationship. The challenge of managing extranets that provide such access increases with the levels and numbers of access granted. In addition to securing sessions over the Web, organizations need a robust authentication and access control mechanism that allows users to gain easy entry to necessary internal resources they need to do their work. The technologies to provide access and authorisation to external users are summarised under the term EAM.

- **ECM – Electronic Countermeasures / ECCM – Electronic Counter-Countermeasures**

  Electronic countermeasures (ECM) are designed to decoy or deceive enemy radar or missile threats. Electronic Counter-Countermeasures (ECCM) are powerful electronics that can 'burn through' conventional ECM systems.

- **FHSS – Frequency-Hopping Spread Spectrum**

  Frequency-hopping spread spectrum (FHSS) is a transmission technology, based on spread spectrum radio where the data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. The transmission frequencies are determined by a spreading, or hopping, code. The receiver must be set to the same hopping code and must listen to the incoming signal at the right time and correct frequency in order to properly receive the signal.

- **GPS – Global Positioning System**

  GPS, run by the Department of Defence of the United States, is a service to acquire two or three dimensional the absolute positions of a receiver on the earth. For the positioning purpose 50 GPS-satellites are used today. To determine a two dimensional position the identifier of three satellites, their position when sending the signal and the time this signal needed to reach receiver are used. The accuracy of the positioning for civilian users today is about ± 15m.

- **GPRS – General Packet Radio Service**

  GPRS is a standard for mobile packet oriented data transfer basing on the European standard GSM (Global System for Mobile Communications). Theoretically, a bandwidth of 171.2 kBit/s for data transfer is reachable, limited for technical and organisational reasons in Germany to 56 kBit/s.

- **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).

- **Identity**

  An identity is a set of characteristics representing a subject.

- **IFF – Friend-or-Foe Identification**

  Friend-or-Foe Identification (IFF) is a system using electromagnetic transmissions to which equipment carried by friendly forces automatically responds, for distinguishing themselves from enemy forces.

- **LED – Light Emitting Diode**

  A LED is a semiconductor diode that converts applied voltage to light. It is used in digital displays, in for example a mobile phone.

- **MMS – Multimedia Message Service**

  Multimedia Messaging Service is a service for exchanging multimedia content between capable mobile phones and other devices.

- **Mobile ID**

  A mobile ID is the ID of a mobile device. The mobile device is typically bound to an individual. Examples in the GSM network are the IMEI (International Mobile Station Equipment), the IMSI (International Mobile Subscriber Identity) and the SIM card (Subscriber Identity Module).

- **Mobile Identity**

  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.

- **Mobile Identity Management**

  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.

- **Mobile Identity Management System**

  A mobile identity management system is a technology-based application for mobile identity management.

- **MOC – Match On Card**

  It means that for a biometric verification process the reference template, the matching algorithm and the matching score decision are all enclosed in the processor chip of a smart card. Only the measurement of the biometric feature and the feature extraction to obtain a query-template are processed outside the card. To authenticate a person the card has to be connected to the external measurement device, which delivers the pre-processed data into the card. Usually the card works only together with dedicated sensor equipment and has proprietary data exchange formats.

- **OASIS – Organization for the Advancement of Structured Information Standards**

  OASIS is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The consortium produces Web services standards along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 4,000 participants representing over 600 organizations and individual members in 100 countries.

- **OTP – One Time Password**

  A one time password is a password that is generated ad-hoc at the moment of an authentication process. There are basically three technologies that use OTP.

  - Time based OTP generators combine a base secret with a time stamp to generate a unique OTP. Both parties of such an authentication scheme have to share the secret and rely on a common time within a certain temporal window.
  - Event-based OTP generators combine a base secret with a counter algorithm to generate a unique OTP. Both parties have to share the secret and use the same algorithm in a way that after each authentication process both parties are able to generate the next accepted OTP in the sequence. In general the receiver will accept an OTP within a few event steps ahead of the last successful communication.

  CR based OTP are used in form of random or specific information coding string that is generated by the authenticating instance ad hoc. They are exchanged between sender and receiver through a CR protocol (see CR)

- **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.

- **Payment Token**

  Specific security token representing payment-related claims.

- **PDA – Personal Digital Assistant**

  A PDA is a small hand-held, usually pen-based, computer. It is often used as a personal organizer.

- **PET – Privacy Enhancing Technologies**

  Privacy Enhancing Technologies (PET) are a related aggregate of "Information and Communications Technology" (ICT) measures protecting personal privacy by eliminating or reducing personal data or by preventing unnecessary or undesired processing of personal data, all without the loss of the functionality of the information system.

- **PICS – Platform for Internet Content Selection**

  PICS is a specification that enables labels (metadata) to be associated with Internet content. Though originally designed to help parents and teachers control what children access on the Internet, it also facilitates other uses for labels, including code signing and privacy.

- **PKI – Public Key Infrastructure**

  PKI (Public Key Infrastructure): The architecture, organization, 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.

- **PRIME – Privacy and Identity Management for Europe**

  PRIME is a European RTD Integrated Project under the FP6/IST Programme. It addresses research issues of digital identity management and privacy in the information society.

- **Peer-to-Peer (P2P)**

  A peer-to-peer (P2P) computer network is any network that does not rely on dedicated servers for communication but instead mostly uses direct connections between clients (peers). A pure peer-to-peer network does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both clients and servers to the other nodes on the network (Wikipedia, 2005).

- **P3P – 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 use of their personal information on Internet sites they visit.

- **RF, RFID, RFID-NIC – Radio Frequency Identification – Near Field Communication**

  RF or RFID is a technology that allows a simple communication between a non powered device with a digital processor (tag) and a powered device (reader). The powered reader generates an electromagnetic field in a selected radio frequency band (e.g. 125 kHz or 13.56 MHz). This field activates and powers the tag through induction (LC-resonant circuit) whenever the tag moves near the source of the field. The tag has an antenna optimised for the specific sender frequency and a small chip that can process the reader request and send answers to the reader. The basic standards for the technology are ISO

10536 (Close Coupling), ISO 14443 (Proximity Coupling), ISO 15693 (Vicinity Coupling) und ISO 18092 (Near Field Communication).

- **SAML – Security Assertion Markup Language**

  SAML was developed by the Security Services Technical Committee of OASIS. It is an XML-based framework for communicating user authentication, entitlements and attribute information. SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject to other entities, which may be a partner company, another enterprise application etc.

  SAML is a flexible and extensible protocol designed to be used by other standards. The Liberty Alliance, the Internet2 Shibboleth project, and OASIS Web Services Security (WS-Security) have all adopted SAML as a technological underpinning to varying degrees. Keys to the federation of identities are standardized mechanisms and syntax for the communication of identity information between the domains – the standard provides the insulating buffer. SAML defines just such a standard.

- **Security Token**

  A security token represents a collection (one or more) of claims. A claim is a declaration made by an entity (e.g. name, identity, key, group, privilege, capability, etc.

- **SIM – 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.

- **SOAP – Simple Object Access Protocol**

  SOAP is an XML-based lightweight protocol for exchange of information in a decentralized, distributed environment. It uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation specific semantics.

- **SMS – Short Message Service**

  Short Message Service is a service for sending messages of up to 160 characters to mobile phones that use GSM communication.

- **SW-or-HW-Token – Software or Hardware Token**

  A SW or HW token in the context of authentication is a carrier for identity credentials. The token may be carried and delivered by a person or a machine to submit a credential for an identity. Examples are digital certificates (SW-token) or digital identity cards (HW-token).

- **UDDI – Universal Description, Discovery and Integration**

  UDDI is a Web-based distributed directory that enables businesses to list themselves on the Internet and discover each other, similar to a traditional phone book's yellow and white pages. It will benefit businesses of all sizes by creating a global, platform-independent, open architecture for describing businesses and services, discovering those

businesses and services, and integrating businesses using the Internet. Any kind of service can be registered in the UDDI Business Registry, such as manual services and electronic services, but the primary intent behind UDDI is to provide a global registry for Web Services.

- **UMTS – Universal Mobile Telecommunications System**

  Universal Mobile Telecommunications System (UMTS) is one of the third-generation (3G) mobile phone technologies. It uses W-CDMA as the underlying standard, is standardized by the 3GPP, and represents the European answer to the ITU IMT-2000 requirements for 3G Cellular radio systems. UMTS is sometimes marketed as 3GSM, emphasizing the combination of the 3G nature of the technology and the GSM standard which it was designed to succeed.

- **USIM – Universal Subscriber Identity Module**

  USIM cards are subscriber identity modules for 3G mobile telephony. They are the same physical size as normal 2G GSM SIM cards.

- **UWB – Ultra-Wide Band**

  Ultra-wide band (UWB) is an emerging wireless technology that uses pulsed radio techniques to transmit data. The transmitter sends a low-power broadband signal, with each channel from 10 to 40 million pulses per second. UWB also has applications in radar systems, including systems that can detect people through walls or rubble.

- **Virtual Identity**

  Virtual identity is sometimes used in the same meaning as digital identity or digital partial identity, but because of the connotation with "unreal, non-existent, seeming" the term is mainly applied to characters in a MUD (Multi User Dungeon), MMORPG (Massively Multiplayer Online Role Playing Games) or to avatars.

- **WAP – Wireless Application Protocol**

  Wireless Application Protocol (WAP) is an open international standard for applications that use wireless communication, for example Internet access from a mobile phone. WAP was designed to provide services equivalent to a Web browser with some mobile-specific additions, being specifically designed to address the limitations of very small portable devices. However, during its first years of existence WAP suffered from considerable negative media attention and has been criticised heavily for its design choices and limitations.

- **WLAN – Wireless Local Area Network**

  A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier: the last link with the users is wireless, to give a network connection to all users in a building or campus. The backbone network usually uses cables.

- **WSDL – Web Service Description Language**

  WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are

combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate.

- **WSS – Web Services Security**

  WSS is a set of standards and recommendations of the OASIS Web Services Security Technical Committee that delivers a technical foundation for implementing security functions such as integrity and confidentiality in messages implementing higher-level Web services applications.

- **XML – eXtensible Markup Language**
  XML describes a class of data objects called XML documents and partially describes the behaviour of computer programs which process them.

8 References

Alkassar, A. and Stüble, C. Towards secure IFF: preventing mafia fraud attacks. In MILCOM 2002. 21st Century Military Communications Conference, volume 2, pages 1139–1144, Anaheim, CA, Oct. 2002. IEEE.

Alkassar, A. and Wetzel, S. An Untraceable Coin-based Incentive Scheme for Multi-Hop Networks. Stevens Technical Report, Stevens Institute of Technology, New Jersey, U.S.A, September 2004.

Alkassar, A., Sadeghi, A.-R. and Stüble, C. Secure Object Identification – Or: Solving the Chess-Grandmaster Problem. In ACM Press: Proceedings of the New Security Paradigms Workshop, Ascona, Switzerland, 2003.

Anderson, R. Onion Routing Information, in R. Anderson (Ed). "Information Hiding", LNCS 1174, Springer Verlag, Berlin, 1996.

Andersson, C.; Fischer-Hübner, S. and Lundin, R. Enabling Anonymity in the Mobile Internet using the *mCrowds* Approach. In: Proceedings of IFIP WG 9.2, 9.6/11.7 Summer School on Risks and Challenges of the Network Society. Karlstad, Sweden. August 2003.

Andersson, C., Lundin, R. and Fischer-Hübner, S. Privacy Enhanced WAP Browsing with *mCrowds*: Anonymity Properties and Performance Evaluation of the *mCrowds* System, Proceedings of the ISSA 2004 Conference, Johannesburg, 30 June - 2 July 2004.

Article 29 Data Protection Working Party (2004) Work Package 100, Opinion on More Harmonised Information Provisions", available at: <http://europa.eu.int/comm/ internal_market/privacy/workingroup/wp2004/wpdocs04_en.htm>.

Balfanz, D. Usable Access Control for the World Wide Web. ACSAC, pp. 406-415, 2003.

Ben Salem, N., Buttyan, L., Hubaux, J. P and Jakobsson, M. A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks. In Proceedings of MobiHOC, 2003.

Bengio, S., Brassard, G., Desmedt, Y. G., Goutier, C. and Quisquater, J.J. Secure implementation ofidentification systems. Journal of Cryptology, 4(3):175–183, 1991.

Bennett, K. and Grothoff, C. GAP - Practical Anonymous Networking. In: International Workshop on Privacy Enhancing Technologies, PET 2003. Lecture Notes in Computer Science: Springer-Verlag GmbH. p.141-160. Dresden, Germany. March 2003.

Berthold, O., Federrath, H. and Köpsell, S. Web MIXes: A System for Anonymous and Unobservable Internet Access. Pubslihed in Lecture Notes in Computer Science, Springer Verlag, 2009:115-129, 2001.

Berthold, O, Federrath, H. and Köhntopp, M. Project 'Anonymity and Unobservability in the Internet'. In *Workshop on Freedom and Privacy by Design / Conference on Freedom and Privacy 2000*, S. 57-65, Toronto/Canada, April 2000.

Beslay, L. and Hakala, H. Digital territories: bubbles, to be published *in the Vision Book*, 2005.

Beth, T. and Desmedt, Y. Identification tokens — or: Solving the chess grandmaster problem. In A. Menezes and S. Vanstone, editors, Advances in Cryptology – CRYPTO '90, volume

537 of Lecture Notes in Computer Science, pages 169–176. International Association for Cryptologic Research, SpringerVerlag, Berlin Germany, 1991.

Brands, S. An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323, Centrum voor Wiskunde en Informatica, March 1993.

Brands, S. and Chaum, D. Distancebounding protocols. In T. Helleseth, editor, Advances in Cryptology – EUROCRYPT '93, volume 765 of Lecture Notes in Computer Science, pages 344–359. International Association for Cryptologic Research, SpringerVerlag, Berlin Germany, 1994.

Brown, Z. Cebolla: Pragmatic IP Anonymity. In: Proceedings of the Ottawa Linux Symposium. p.55-65. Ottawa, Ontario, Canada. June 2002.

Buchegger, S. and Le Boudec, J. Y. Performance analysis of the confidant protocol (cooperation of nodes -fairness in dynamic ad hoc networks). In Proceedings of MobiHoc 2002, Lausanne, June 2002.

Buchmann, J., Ruppert, M. and Tak, M. FlexiPKI - Realisierung einer flexiblen Public-Key-Infrastruktur. Technical Report, TU Darmstadt, December 1999.

Buttyan, L. and Hubaux, J. P. Enforcing service availability in mobile ad hoc wans. In Proceedings of IEEE/ACM Workshop on Mobile AdHoc Networking and Computing (MobiHOC), Boston, MA, USA, August 2000.

Buttyan, L. and Hubaux, J. P. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applications, 8(5), October 2003.

Cabrera, L.F., Kurt, C. and Box, D. An Introduction to the Web Services Architecture and Its Specifications. Version 2.0. October 2004. http://msdn.microsoft.com/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnwebsrv/html/introwsa.asp.

Chaum, D. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. In: Communications of the ACM, v.24, i.2, Feb. 1981, p.84-90. New York, New York, U.S.A.: ACM Press, 1981.

Chaum, D. The dining cryptographers problem: unconditional sender and recipient untraceability, Journal of Cryptology, pp 65-75, 1 (1), 1988.

Claessens, J., Preneel, B. and Vandewalle, J. Combining World Wide Web and wireless security. Informatica, 26(2):123–132, July 2002.

Claessens, J. Analysis and design of an advanced infrastructure for secure and anonymous electronic payment systems on the Internet. Ph.D. thesis, K.U.Leuven. December 2002.

Denning, D. and MacDoran, P. Location-based Authentication: Grounding Cyberspace for Better Security, Computer Fraud and Security, pages 167-174, Elsevier Science, February 1996.

Desmedt, Y. Major security problems with the 'unforgeable' (feige)fiatshamir proofs of identity and how to overcome them. In SecuriCom '88, SEDEP Paris, France, 1988.

Dingledine, R., Mathewson, N. and Syverson, P. Tor: The Second Generation Onion Router. Published in Proceedings of the 13th USENIX Security Symposium, San Diego, USA, 2004.

Escudero-Pascual, A., Heidenfalk, M. and Heselius, P. Flying Freedom: Location Privacy in Mobile Internetworking. Published in Proceedings of INET 2001, Stockholm, Sweden, 2001.

Escudero-Pascual, A., Holleboom, T. and Fischer-Hübner, S. Privacy of Location Data in Mobile Networks. Published in Proceedings of the Nordsec 2002, Karlstad, Sweden, 2002.

FDA, COMBATING COUNTERFEIT DRUGS, A Report of the Food and Drug Administration (USA), February 2004.

Figge, S. Situation dependent m-commerce applications. Proceedings of the Conference on Telecommunications and Information Markets, Kingston, 2001

Figge, S. et. al.: EARNING M-ONEY - A Situation based Approach for Mobile Business Models, In: Proceedings of the 11th European Conference on Information Systems (ECIS); Naples, Italy, 2003

Fischer-Hübner, S. IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms. Lecture Notes in Computer Science, vol.1958. Springer-Verlag Berlin Heildelberg. 2001. 351p.

Fischer-Hübner, S., Nilsson, M. and Lindskog, H. Self-Determination in Mobile Internet, Proceedings of IFIP TC11 17th International Conference on Information Security (SEC 2002), Cairo/Egypt, 7-9 May 2002, Kluwer, Academic Publishers., 2002.

Freedman, M.J. and Morris, R. Tarzan: A Peer-to-Peer Anonymizing Network Layer. In: Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002). Washington, DC, USA. November 2002.

Gerd tom Markotten, D. and Kaiser, J. Benutzbare Sicherheit – Herausforderungen und Modell für E-Commerce-Systeme. In: Wirtschaftsinformatik, Vol. 6, pp. 531-538, December 2000.

Gerd tom Markotten, D., Jendricke, U. and Müller, G. Benutzbare Sicherheit - Der Identitätsmanager als universelles Sicherheitswerkzeug. In Günter Müller und Martin Reichenbach (Eds.), Sicherheitskonzepte für das Internet, Kapitel 7, S. 135-146. Springer-Verlag Berlin, May 2001.

Gerd tom Markotten, D., Wohlgemuth, S. and Müller, G. Mit Sicherheit zukunftsfähig. PIK Sonderheft Sicherheit 2003, 26(1):5-14, 2003.

Gerd tom Markotten, D. Benutzbare Sicherheit in informationstechnischen Systemen. RHOMBOS-Verlag, Berlin, 2004.

Girard, J., Hirst, C., Mobile Authentication Yields Anytime, Anywhere Control, Gartner Research Group report; G00123588; October 2004.

Goel, S. et al. Herbivore: A Scalable and Efficient Protocol for Anonymous Communication. In: Cornell University Computing and Information Science Technical Report, TR2003-1890, 17p. Ithaca, New York, U.S.A. February 2003.

Hansen, M., Krasemann, H., Krause, C., Rost, M. and Genghini, R. Identity Management Systems (IMS): Identification and Comparison Study, p. 82 – 83, Seville 2003; download: http://www.datenschutzzentrum.de/projekte/idmanage/study.htm

IBM Corporation and Microsoft Corporation. Secure, Reliable, Transacted Web Services: Architecture and Composition. September 2003.

http://msdn.microsoft.com/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnwebsrv/html/wsoverview.asp.

IBM Corporation and Microsoft Corporation. Federation of Identities in a Web Services World. Version 1.0. July 8, 2003. http://msdn.microsoft.com/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnglobspec/html/ws-federation-strategy.asp.

Jakobsson, M. Buttyan, L. and Hubaux, J. P. A micro-payment scheme encouraging ollaboration in multi-hop cellular networks. In Proceedings of the Fourth Conference on Financial Cryptography (FC'03), Lecture Notes in Computer Science, pages 15–33, Hamilton, Bermuda, Springer-Verlag, Berlin Germany, 2003.

Jakobsson, M. , Capkun, S. and Hubaux, J. P. Secure and privacy-preserving communication in hybrid ad hoc networks. Technical Report IC/2004/10, EPFL-DI-ICA, January 2004.

JAP Web Mixes, http://anon.inf.tu-dresden.de/, accessed 21 November 2003.

Jendricke, U. and Gerd tom Markotten, D. Usability meets Security - The Identity-Manager as your Personal Security Assistant for the Internet. In Proceedings of the 16th Annual Computer Security Applications Conference, pages 344-353, December 2000.

Jendricke, U. and Gerd tom Markotten, D. Identitätsmanagement: Einheiten und Systemarchitektur. In Dirk Fox, Marit Köhntopp and Andreas Pfitzmann (Hrsg.), Verlässliche IT-Systeme - Sicherheit in komplexen Infrastrukturen, S. 77-85. Vieweg, Wiesbaden, September 2001.

Jendricke, U., Kreutzer, M. and Zugenmaier, A. Mobile Identity Management. Technical Report 178, Institute fuer Informatik, Universität Freiburg, October 2002. Workshop on Security in Ubquitous Computing, UBICOMP 2002.

Jiejun Kong, X. H. Andor: Anonymous on demand routing with untraceable routes for mobile ad hoc networks. In Fourth ACM International Symposium on Mobile AdHoc Networking and Computing (MobiHoc'03), pages 291–302, 2003.

Levine, B.N. and Shields, C. Hordes: a multicast based protocol for anonymity. In: ACM Journal of Computer Security. v.10, i.3, 2002. p.213-240. Amsterdam, The Netherlands: IOS Press, 2002.

Marti, S., Giuli, T., Lai, K. and Baker, M. Mitigating routing misbehaviour in mobile ad hoc networks. In Proceedings of the sixth annual International Conference on Mobile Computing and Networking, pages 255–265, Boston MA, USA, Aug. 2000.

Michiardi, P. and Molva, R. CORE: a collaborative reputation mechanism to en-force node cooperation in mobile ad hoc networks. In CMS'2002, Communication and Multimedia Security 2002 Conference, Portoroz, Slovenia, August 2002.

Microsoft Corporation and Vodafone Group Services Ltd. Mobile Web Services: Convergence of PC and Mobile Applications and Services. November 2003. http://www.microsoft.com/serviceproviders/mobilewebservices/mws_whitepaper.asp.

Microsoft Corporation and Vodafone Group Services Ltd. Mobile Web Services Technical Roadmap. November 2003. http://www.microsoft.com/serviceproviders/mobilewebservices/mws_tech_roadmap.asp.

Mislove, A. et al. AP3: Cooperative, Decentralized Anonymous Communication. In: Proceedings of the 11th ACM SIGOPS (Special Interest Group on Operating Systems) European Workshop (EW'04). Leuven, Belgium. September 2004.

Müller, G. and Stapf, K.H. Mehrseitige Sicherheit in der Kommunikationstechnik. Vol. 2. Erwartung, Akzeptanz, Nutzung, Addison-Wesley, Bonn, 1998.

Müller, L., Jacomet, M., Cattin, R., Dispositif de sécurité pour transaction en ligne, Patentschrift EP1255178 , 2002.

Narten, T. and Draves, R. Privacy Extensions for Stateless Autoconfiguration in IPv6, RFC3041, January 2001. Accessed at http://www.ietf.org/rfc/rfc3041.txt on June 21, 2002.

Nilsson, M., Lindskog, H. and Fischer-Hübner, S. Privacy Enhancements in the Mobile Internet, Proceedings of IFIP WG 9.6/11.7 working conference on Security and Control of IT in Society, Bratislava, 15 -16 June 2001.

Papadimitratos, P. and Haas, Z. In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS2002), San Antonio, TX, Jan. 2002.

Pettersson, J. S. P3P and Usability – the Mobile Case. In Duquennoy, P., S. Fischer-Hübner, J. Holvast & A. Zuccato (eds.) Risk and challenges of the network society, Karlstad University Studies 2004:35., 2004.

Pettersson, J. S., ed. (2004b) D06.1.a: General mock-ups, confidential deliverable from the PRIME project (www.prime-project.eu.org/)

Pfitzmann, A. and Hansen, M. Anonymity, Unobservability, Pseudonymity, and Identity Management – A Proposal for Terminology v0.21, 2004. Accessed at http://dud.inf.tu-dresden.de/Literatur_V1.shtml, February 2004.

P3P 1.0 element definitions and translations - 27 November 2003 Draft, available at <http://www.w3.org/P3P/2003/11-p3p-translation.htm>.

P3P The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, W3C Working Draft 20 July 2004, http://www.w3.org/TR/2004/WD-P3P11-20040720/

Rannenberg, K., Pfitzmann, A. and Müller, G. Sicherheit, insbesondere mehrseitige IT-Sicherheit. In Günter Müller und Andreas Pfitzmann (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, S. 21-29. Addison-Wesley Longman Verlag GmbH, 1997.

Reiter, M. and Rubin, A. Crowds: Anonymity for Web Transactions. Published in DIMACS Technical report, 97-15, 1997.

Reiter, M. and Rubin, A. Crowds: Anonymity for Web Transactions, ACM Trans. On Information and Systems Security, pp 66-92, 1 (1), 1998.

Reiter, M. and Rubin, A. Anonymous Web transactions with Crowds. In: Communications of the ACM. v.42, i.2, Feb. 1999, p.32-48. New York, New York, USA: ACM Press, 1999.

Rennhard, M. and Platter, B. Introducing MorphMix: Peer-to-Peer based Anonymous Internet usage with Collusion Detection. In: Proceedings of the Workshop on Privacy in Electronic Society (WPES). Washington, DC, USA. Nov. 2002.

Reynolds, F., Hjelm, J., Dawkins, S. and Singhal, S. CC/PP: A user side framework for content negotiation. W3C Note, URL: http://www.w3.org/TR/NOTE-CCPP/. July 1999.

Shapiro, C. and Varian, H.R.: Information Rules, Harvard Business School Press (Boston) 1999

Sherwood, R., Bhattacharjee, B. and Srinivasan, A.. P5: A Protocol for Scalable Anonymous Communication. In: Proceedings of the 2002 IEEE Symposium on Security and Privacy. Washington, D.C., U.S.A: IEEE Computer Society. p.58-70. Berkeley, California, U.S.A. May 2002.

Sedov, I., Haase, M., Cap, C. and Timmermann, D. Hardware Security Concept for Spontaneous Network Integration of Mobile Devices. In Proceedings of the International Workshop "Innovative Internet Computing Systems", Ilmenau, June 2001.

Simon, H.A. Models of Man - Social and Rational. John Wiley & Sons, New York 1957.

Syverson, P. F., Goldschlag, D. M. and Reed, M. G. Anonymous connections and onion routing. In Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, CA, May 1997. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press.

UAProf, WAP-174: WAG UAPROF User Agent Profile Specification. Wireless Application Group. http://www1.wapforum.org/tech/terms.asp?doc=SPEC-UAProf-19991110.pdf

Waidner, M. Open Issues in Secure Electronic Commerce. Technical Report, IBM Research Division, Zürich, October 1998.

Waidner, M. and Pfitzmann, B. Unconditional Sender and Recipient Untraceability in spite of Active Attacks – Some Remarks, Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 5/89, March 1989. Accessed at http://www.semper.org/sirene/publ/WaPf_89IB_DCandFailStop.ps.gz, on May 24, 2002.

Weiser, M., "The computer for the Twenty-First Century", Scientific American 165, 1991, p. 94-104.

Westin, A. F., *Privacy and Freedom*. Atheneum, New York, NY. 1967

Whitten, A. and Tygar, J.D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: Proceedings of the 8th USENIX Security Symposium, August 1999.

Wikipedia - the free encyclopedia. Accessed in: http://en.wikipedia.org/wiki/Peer-to-peer, on February 16, 2005.

Wohlgemuth, S., Gerd tom Markotten, D., Jendricke, U. and Müller, G. DFG-Schwerpunktprogramm "Sicherheit in der Informations- und Kommunikationstechnik". it – Information Technology, 45(1):46-54, 2003.

Wolf, G. and Pfitzmann, A. Properties of protection goals and their integration into a user interface. Computer Networks, 32:685-699, 2000.

World Wide Web Consortium (W3C), Composite Capability/Preference Profiles (CC/PP): Structure and Vocabularies 1.0, W3C Recommendation 15 January 2004, http://www.w3.org/TR/2004/REC-CCPP-struct-vocab-20040115/

Ying-Dar Jason Lin, Y.-C. H. Multihop cellular: A new architecture for wireless communications. In INFOCOM2000, volume 3, pages 1273–1282. IEEE, 2000.

Zhong, S. Chen, J. and Yang, Y. R. Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks. In Proceedings of IEEE INFOCOM'03, San Francesco, CA, April

2003.

Zhu, Y. and Hu, Y.. TAP: A Novel Tunneling Approach for Anonymity in Structured P2P Systems. In: Proceedings of the 2004 International Conference on Parallel Processing (ICPP 2004). Montreal, Quebec, Canada. August 2004.

Zugenmaier, A. Anonymity for Users of Mobile Devices through Location Addressing, Rhombus-Verlag, Berlin, 2003.