universität wien

DISSERTATION

Titel der Dissertation

"Privacy in Location-Based Services"

Verfasser

Mag. Oliver Jorns

angestrebter akademischer Grad

Doktor der Technischen Wissenschaften (Dr. techn.)

Wien, im August 2009

Studienkennzahl lt. Studienblatt:	A 786 881
Dissertationsgebiet lt. Studienblatt:	Informatik
Betreuer:	O.Univ.-Prof. DDr. Gerald Quirchmayr

To my wife Ulrike and my children Laurin and Annika

Contents

List of Figures

List of Tables

Abstract

During the last years the development of mobile devices has gained significant progress with respect to memory capabilities, advanced processing power and higher transfer rates to name only a few performance parameters. At the same time eclectic positioning and localization technologies are meanwhile mature enough to be integrated into mobile devices. Not until positioning, localization and telecommunication technologies can be combined, seamlessly the basis for the proliferation of a new generation of context-aware applications and business models can be build. In this respect, location and position information foster novel future context-aware applications. But, if this information is in the wrong hands such applications may by the same token pose severe threat. Therefore, apart from technical means against attacks, forgery and misuse of sensitive user information the interaction of all these systems must comply with legal requirements that precisely prescribe all aspects of telecommunication systems. In this spirit, the main research objective addressed for the design of new context-aware and location-based systems must be the protection of the user's privacy.

This dissertation discusses first various aspects of location-based systems and out of it the various needs that have to be addressed to be able to provide flexible location-based services to mobile users by preserving privacy. The main contribution of this work is a mechanism that is based on the notion of pseudonyms. The use of this kind of pseudonyms provides maximum security and privacy for users during communication.

The second contribution is a telecommunication service architecture that is tightly coupled with the pseudonym mechanism. It allows new business models to be applied by leveraging the use of some services of the telcos' infrastructure. This service application further allows the implementation of the so called pay-as-you-go concept. This allows customers to anonymously consume mobile services that are offered by third party application providers similarly to buying physical goods with cash.

Finally, we demonstrate the implementation of a service platform that allows us to illustrate the operation of the pseudonym mechanism and the interworking of the system architecture's components that are tailored for the realization of location-based applications.

Kurzfassung

Während der letzten Jahre erfuhren mobile Geräte durch grössere Speicher, der Entwicklung schnellerer Prozessoren und höherer Übertragungsraten, um nur einige der wichtigsten Performanceparameter zu nennen, einen enormen Entwicklungsschub. Gleichzeitig sind die unterschiedlichen Positionierungssysteme mittlerweile ausgereift und klein genug, um in mobile Geräte verbaut werden zu können. Erst durch die Möglichkeit der Zusammenführung von solchen ausgereiften Positionierungs- mit existierenden Telekommunikationstechnologien kann die Basis für eine neue Generation kontextsensitiver Anwendungen und entsprechender Geschäftsmodelle geschaffen werden. Abgesehen von den technischen Massnahmen die zum Schutz gegen Attacken, Verfälschungen und Missbrauch sensitiver Daten eingesetzt werden, müssen diese auch allen rechtlichen Aspekten und Rahmenbedingungen von Telekommunikationssystemen entsprechen. In diesem Sinne muss das Ziel von Forschungen im Bereich neuer kontext-sensitiver Systeme und Anwendungen die mit Positionsdaten operieren der Schutz der Privatheit jedes einzelnen Nutzers sein.

Diese Dissertation beginnt mit einer Diskussion über verschiedene Aspekte von Location-Based Systemen. Es werden weiters unterschiedliche Anforderungen aufgezeigt deren Erfüllung notwendig sind, um flexible Systeme anbieten zu können und die zudem den Schutz der Privatheit der Nutzer garantieren können. Der wohl wichtigste Beitrag dazu ist ein Mechanismus der auf dem Begriff des Pseudonyms basiert. Dieses Verfahren garantiert maximale Sicherheit und Schutz der Privatheit der Benutzer während der Nutzung von Diensten.

Der zweite Beitrag der Dissertation ist eine Telekom Service Architektur die den erwähnten Pseudonym-basierten Mechanismus integriert. Durch Einbeziehen dedizierter Dienste von Telekommunikationsanbietern bildet diese Architektur die Basis für die Realisierung neuer Geschäftsmodelle und ermöglicht die Implementierung des *pay-as-you-go* Konzeptes. Dieses ermöglicht Kunden anonym mobile Dienste von Drittanbietern zu konsumieren, ähnlich dem anonymen Kauf von Gütern mit realem Geld.

Schliesslich wird mit der Implementierung einer Service Platform sowohl die Funktionsweise des Pseudonym Mechanismus sowie die Interaktionen der in der System Architektur vorgesehenen Dienste und Komponenten die zur Realisierung von Location-Based Anwendungen bentigt werden demonstriert.

Acknowledgements

I want to thank my supervisor, Gerald Quirchmayr who is the head of the Department of Distributed and Multimedia Systems at the University of Vienna and Adjunct Professor at the School of Computer and Information Science of the University of South Austrialia. During the development and writing of my dissertation I was pleased that he spent very much of his time for valuable discussions which in turn motivated me to exceed my results anew. The resulting teamwork allowed us to publish a reasonable number of international conference papers, a journal paper and a book section. In addition to fostering my publication skills I was from the beginning on also invited to take over lectures which allowed me to continue my teaching path which I constantly keep up.

I also want to thank my friends and colleagues from the Department of Knowledge and Business Engineering at the University of Vienna, especially Erich Schikuta who is the second advisor of this work. He also helped me many times to stay in close touch with the academic community which further allowed me to not only develop my teaching skills but also participate in new and exciting research disciplines. Furthermore I want to thank Peter Beran, Jürgen Mangler, Martin Polaschek and Helmut Wanek. With all of them I enjoyed both, scientific work and additionally much fun which I hope continues.

I also want to thank my colleagues at ftw. Slobodanka Tomic for valuable discussions, Joachim Zeiss for his calm nature, his inspiring ideas and discussions and the continuing cooperation. I also want to thank very much Hans-Peter Schwefel from Aalborg University in Denmark who is the Scientific Director at ftw. His valuable suggestions and feedback on core chapters of this thesis helped me to clarify some important aspects of this thesis. Sandford Bessler and Rudi Pailer with whom I developed the main features of the proposed pseudonym generation scheme which was first patented and resulted a few years later in my thesis. Finally, I want to thank René Gabner and all the other colleagues I met at ftw. namely Julia Gross, Oliver Jung and Barbara Stähle with whom I had the chance to work on new ideas.

Chapter 1

Introduction

The ongoing fusion of internet technologies and its manyfold services with telecommunication technologies that are part of globally connected mobile networks is challenged by continuous large-scale changes. The last decade showed that the accelerated development of different technologies on the one hand enhances the quality and performance of networks but on the other hand also reduces the life-cycle thereof. As a result many developments are outdated even before they enter the market which means that technological decisions bear risks and costs likewise. *Location-Based Services* (LBS) are such an example that clearly shows how early overcast expectations soon experienced disappointment. The example also shows, that some developments and technologies bear huge potential which can be utilized later in different ways with huge impact.

For the development of LBS many important technical bases such as GPS were in place even long before. Anyhow, it took more than one decade and huge efforts to make the vision of mobile computing true and with it useable LBS as we can see them today. Having overcome the most technical obstacles that prevented LBS from being accessed and used only a decade ago, the meanwhile widespread use of LBS also raises a number of important questions that are for the most part still unanswered. The example of LBSs shows how different technologies not only influence the behavior of individuals or groups. It also shows that such tremendous changes affect even nations and the whole society.

From the network operator's point of view the opening of mobile networks and the penetration of internet technologies provide not only new opportunities but also the risk of introducing new threads that they so far did not have to take care of. By the same token users and customers exchange and share an unprecedented amount of data. This includes also data that is private or can be classified as to be privacy sensitive. The maturation and fusion of different technologies and the changing way networks and services are used raises challenges for different research communities. In the light of this complex development research in the area of Location-Based Services investigates one important challenge: How to protect the user's location data and guarantee location privacy?

Besides different possible means that aim to protect the user's location privacy the European Community claims the development of Privacy Enhancing Technologies. Here, the objective is *data protection*. In this respect *anonymity* and *pseudonymity* play a fundamentally important role [13] (L 201/38). Accordingly, in this dissertation we investigate the use

of pseudonyms. As pseudonyms are usually permanent, that means it is either not possible or intended to change the pseudonyms its, usefulness is basically limited if not questionable. The use of permanent pseudonyms is accompanied with the adaption of the pseudonym as part of the real identity. Roughly speaking, over time pseudonyms become part of the real identity. The possibility that the real identity can be revealed with relatively less effort renders permanent pseudonyms rather useless [14] (p. 30). Other attempts that propose to change pseudonyms sometimes provide just as little protection.

1.1 Contributions of this Dissertation

This dissertation provides several contributions to the research field of privacy in Location-Based Services which are mainly represented by the following three core topics:

The core contribution is a new pseudonym generation scheme. Pseudonyms represent amongst others one important Privacy Enhancing Technology. But, the use of permanent pseudonyms is problematic since they cannot protect the individuals identity information and location privacy et all. Unlike other pseudonym based solutions that at the best consider only irregular or explicitly induced changes, we propose a novel scheme that guarantees with only little effort not any equal pseudonym.

The penetration of the mobile market introduces new business models and the development of service architectures. We demonstrate the fusion of telecommunication and internet technologies by applying a dedicated system architecture which allows embedding the pseudonym generation scheme. We derive a business model that further reflects the so called *pay-as-you-go* paradigm. With it, mobile users may consume (mobile) services on the way from untrusted service providers without the hassle of prior registration and with best possible protection of their privacy sensitive data.

We present real-world telecommunication services provided by a network operator which are used for the realization of the service architecture. The implemented platform combines those different services and integrates the proposed pseudonym generation scheme. We explain the message interactions for service consumption as well as dedicated privacy aspects.

The core of the dissertation is rounded down by an application example that demonstrates how an innovative real life application could be extended by location information and the aforementioned means for privacy protection.

1.2 Organization and Outline of this Dissertation

This dissertation is organized as follows:

Chapter 2 This dissertation starts with a discussion about the notion of context, context-awareness and context-aware computing, the relevance of security and privacy and especially, as this is certainly one of the most important context variable, that of location. A comparison between context-aware computing and location-based services is given

which is followed by concerning different location technologies and a classification of currently available location-based services. We also discuss some examples of location-based services and provide an overview of the different underlying design patterns and its relation to location privacy.

Against the background of mobile business we show a holistic view on the different aspects of the mobile market. This includes explanations regarding the different actors in the mobile business, the question what a business model in a mobile business is and some scenarios that are currently met. In this respect we also discuss the proposed system architecture and the combination with the pseudonym generation scheme that allows for privacy protection of mobile users.

Another important part of this chapter is devoted to a general discussion about different aspects of privacy which includes a historical review, the legal situation, especially that of Europe and an overview about the research activities and the relevant literature in this area. Other privacy related questions such as those that relate to standardization work in the area of location privacy, management of privacy and questions in connection with possible vulnerabilities of network operators conclude this chapter.

Chapter 3 gives a brief overview about the underlying cryptographic mechanisms of the proposed pseudonym generation scheme. This includes the requirements and operation as well as a security analysis. The presented cryptographic primitives and security services are essential for the solution development which is discussed from section 4 (p. 91) on.

Authentication is an essential security service and serves as basis for the realization of the pseudonym generation scheme. From a theoretical point of view the security service *authentication* also provides contradictions with other security principles such as *repudiability*, *confidentiality* and *forward security*. Since our proposed pseudonym generation scheme is fundamentally authentication, we ought to consider the conceptions of causal relations. This is of major importance for understanding the basic underlying principles that are inherent to the proposed pseudonym generation scheme. We also explain some exemplary authentication schemes that represent practical realizations of basic security services.

Chapter 4 is divided into two parts. The first part discusses the components the service architecture is composed of. We indicate different trust levels and multiple existing relations that are associated with the deployment of different services that may be operated by different organizations. After the architectural discussion we provide a short review of the basic principles of the pseudonym generation scheme which also includes an illustration and review of the core security aspects. Furthermore, we provide some performance measurements that show that the proposed scheme is applicable also on legacy mobile devices.

Some fundamental operations in the the area of location-based services are discussed in the light of the proposed system architecture and pseudonym generation scheme. In this respect we also discuss the error recovery strategies in case of errors and the allocation of the applications according to the previously identified classification pattern.

The second part of this chapter continues with an in depth discussion of the user registration procedure and the subsequent initialization procedure of the so-called *self-identifying* pseudonyms. This kind of pseudonyms represents the basis of how users authenticate themselves and further serves for the initialization of chains of pseudonyms that refer to user relationships,

Amongst the many possible designs and implementations that aim at realizing secure communication we discuss one dedicated example that is proposed by Borisov et al. [15]. As their solution primarily aims at realizing social communication and we can identify some aspects of our pseudonym generation scheme as being only slightly different, we review this scheme in further detail in section 4.6 (p. 122).

Finally, this section addresses another important issue, that is the exchange of information and combination across different network operator's domains. We show that the pseudonym generation scheme also provides a viable solution when sensitive data shall be accessible even across between different network operator's domains.

Chapter 5 covers the most important implementation aspects of the localization platform. One such part refers to *cell-based* localization which is an intrinsic par of the network operator's infrastructure. We also show how the implemented platform allows the processing of GPX files which can be used to play back previously recorded tracks. This allows for the simulation of multiple mobiles that, depending on the respective application, track herself or, if allowed, other persons.

Generally, this section provides a technical perspective of different technologies that are necessary for the realization of the various parts of the tracking platform. This includes a description of the various processes that are triggered while users and operators interact with the system. By looking at the basic principles of some fundamental network operator's services like e.g. the location service we can derive different location update strategies that are inherently important for the design and implementation of location-based services. At this point we refer to Rasmus L. Olsen [16] who discuss an analytical model for dynamically changing information.

Chapter 6 presents the implementation of a mobile transport ticket research prototype application. Some of the implemented features are made available through the inclusion of location information. We discuss the integration of the tracking platform on a conceptual level and show that popular applications such as transport ticket applications may be extended by such technologies. Based on the experiences we made with this kind of application we also discuss some shortages that are unavoidable through the use of centralized localization. In this spirit we also discuss what implications the inclusion other kinds of localization technologies, namely the opposite of centralized technologies may have. Finally, this example demonstrates the obvious need for privacy protection. The proposed pseudonym generation scheme is one possible means for secure exchange of location data within a real world location-based application.

Chapter 7 wraps up the main message of this disertation and provides further outlook regarding ongoing research.

Chapter 2

Background & State of the Art

In this chapter we highlight some of those underlying basics of this dissertation that are important to gain an overall understanding of the research area. Therefrom the reader may better understand the importance of our contribution. We start with a very general view on context-aware computing which is not only a complex topic on its own and influences today's research and development of location-based services and applications. This discussion involves the research challenges as well as clarifications what context is and how to define it in the light of different technologies and applications. The presented examples of past context-aware applications confirm some of the fundamental findings that are still valid and investigated. One of the most important fundamental question today is how to deal with privacy questions. The importance of this question is out of question since it is of vital importance whether location-based services will be a success in future or not.

2.1 Context-Aware Computing

Various researchers from different areas in computer science are dealing since at least 40 years with the concept of context [17]. The first who introduced the term "*context-aware computing*" were Salber et al. [18] with their work on the *ContextToolkit*, aimed at simplifying the design, implementation and evolvement of context-aware applications [19] (p. 36). As stated by Raper *et al.* [20] they also defined the so called five W's which denote the following questions: *Who is the user and/or the other people around? What the user is doing? Where is the user? When is the usage taking place, including relative time?* and *Why is the user doing what she is doing*? These questions describe the minimal set of necessary contexts and are also referred as the 5 W's defined by [19].

In this respect Mark Weisers seminal paper [21] is meanwhile deemed to be the pioneering vision of ubiquitous computing. By the time of writing the seminal paper, the technology that was required to realize his vision was not available. It took approximately a decade till the necessary technology was actually available and mature enough to be used for the implementation of the first prototypes. One event that certainly directed the attention to context-aware computing in general at this time was the *International Symposium on Handheld and Ubiquitous Computing* (HUC'99) [22] (since 2001 renamed to *Ubicomp*) that fostered the development of research in this area and marked the beginning of a series of conferences

in this field [23]. During this time, a number of early prototypes originated and theoretical examinations resulted in the first definitions of *context-awareness*.

One of these definitions describes a combination of *information appliances* and *awareness*. Whereas information appliance subsumes special purpose devices such as mobile phones, handheld computers and different sorts of embedded systems, the latter allows to actually support users in their daily activities. Thus, awareness requires computer systems to understand the users activities to provide context to the user for which the system operates. While awareness is the key issue for the realization of dynamic, user friendly and supportive environments, the combination with information appliances and, as R. Mayrhofer [23] (p. 2) continues, the implementation of awareness in information appliances is meanwhile known as *context-awareness*.

A rather critical view on context-aware computing not only from a scientific point of view but also from an engineering and usability perspective is presented in the article written by Erickson [24]. He claims that context-awareness the notion of context and context-awareness may in some sense be misleading. In comparison with the human perception of context, the systems context-awareness is very different. Erickson underpins his examination by providing some examples that make these differences obvious. One such example is the comparison of contexts during a visit to a theater. Mobile devices may only sense darkness and motionless and possibly some other parameters. This definitely contrary to what humans perceive in a theater. Other examples such as locking the door if the cars engine is running, starting the screensaver at the end of a presentation or the unsuspected activation of a microphone are representative for indeed ordinary actions that is obviously an knowledge-intensive activity that is, withal difficult to implement. Attempts to induce understanding and making systems more robust simply by adding additional rules or heuristics ultimately leads to more complexity.

Context-aware systems that only react upon changing context information differ from those that are able to predict future user contexts and in that sense act proactively on behalf of the user. R. Mayrhofer [23] shows that through classification of current situations and by extrapolating the past it is possible to forecast future user context.

Human beings normally have no problem to express themselves with natural language and react in the right manner according to certain situations. We also usually have no problem to understand and learn from new situations, even if we do not experience these situations by ourselves. Our knowledge about the surrounding world, the richness of our languages and the ability to draw conclusions allows us to understand and communicate facts and relations that were not understandable without complex scientific models or human intuition. This ability allows us to understand also situations that we do not actually need to experience on our own nor do we solely have to rely on past experiences in order to be able to solve problems and provide adequate solutions.

By using telecommunication systems, almost all the deeply human communication capabilities are only at limited disposal and thus also only a small fraction of the available bandwidth of expression in contrast to as if communicating face to face. However, computers and telecommunication systems allow us to communicate even over long distances and meanwhile in many different ways. So, even if all these technical means of communication may only provide limited means to express ourself, anyhow, it gives us the possibility to communicate in almost every situation and, what is possible since the beginning of telephony, every place even

if we're not on sight. But, telecommunication systems do not only help us to communicate with each other. In general, communication became one of the most important assets in the industrial and information society.

Context, with regard to computer science, is not only a key concept in Human-Computer Interaction, in particular (HCI) in Language Processing. Since the advent of mobile devices about a decade ago, the notion of context awareness underwent a revival in a new domain called *mobile computing* which, during the last years, develops magnificently. The fast adaption and the implementation of the ideas and concepts with regard to the different notions of context was first and foremost given by the possibility of building small, cheap sensors. Especially the telecommunication industry and the ubiquitous computing community took the advantage of this development which, over the years, resulted in a reasonable number of interesting research prototypes and even commercial products.

Whereas in the beginning of the mobile computing area, context-aware systems used mainly location as context, later projects also integrated time as context variable. The fast development of sensor technology evolved the possibilities to gather manyfold contextual information about the physical environment. Today, context aware mobile computing is on the advance.

As already mentioned above, context-awareness is inherent to human beings but hard to implement in computer science. Anyhow, the evolvement of different technologies approaches context aware computing, at least step-by-step as it was envisioned many years before.

2.1.1 Challenges

In his dissertation Mayrhofer [23] (p. 3) provides a list of general challenges that in any case affects research on context. The list includes questions concerning understanding what the concept of context is, how to acquire context and make use out of it, how to connect context acquisition to its use and the influence on human computer interaction. More practical, challenges also include support of context-aware ubiquitous computing systems and their evaluation.

Aside from these general challenges, Mayrhofer explicitly mentions some additional ones that are more specific. The most worthwhile but by the same token also most challenging one is that of context prediction.

In the following a brief overview is given about what constitutes the notion of context. This includes an explanation of the most important context variables just as well as technology that is used to sense. After that, we discuss a particular development that stems from and at the same time is context-aware computing, that is, location-based services and its applications.

2.1.2 What is Context?

There is maybe no general answer to the question what context actually is but there exist many different definitions. In the light of context-aware computing during the last years and in the course of the development of new technologies, researchers extended and refined their definitions of context. The results that were gained about a decade ago from tests with mobile device prototype implementations that were equipped with simple sensor technology

may retrospectively appear very basic. But, as the following closer examinations show, quite the contrary is true.

In the often cited paper by Schmidt et al. [17] two mobile prototypes that use only low-cost sensor technology demonstrate the importance and applicability of adaptive user interfaces. One prototype demonstrates a light-sensitive display, whereas the other one realizes an orientation-sensitive user interface. The use of low-level sensors and data is used by a layered architecture that provides a successive abstraction from measured physical conditions. The researchers aim to figure out which combinations of sensors fit best for the realization of context-awareness, which methods were needed in order to be able to evaluate relations between the sensors and the situations and, finally, answer the question if it is possible to construct even more complex contexts from simpler ones.

A. Dix et al. [25] primarily distinguishes four different kinds of context and provides a taxonomy which includes *infrastructure context*, *system context*, *domain context* and *physical context*. Their consideration of context first concerns the nature of the underlying *infrastructure* to consider the overall *system context*. Then, the consideration of the broader application *domain context* is followed by the actual *physical context* to consider. Particular features of mobile devices are not the decisive factors for the interaction of mobile applications. The realization of mobile applications rather depends on the mobile device and the supporting infrastructure.

Although Dix et al. focus rather on different interaction possibilities for mobile systems, their conception of *infrastructure* comes along with the conception of infrastructure by Chen et al. [26]. They claim that the shift from distributed systems with a stationary execution environment is not suitable for mobile scenarios and that it is wrong to try to simply hide mobility by adapting systems instead of making the effort to explore and provide infrastructure for the development of new mobile applications.

Their definition of context *"Context is the set of environmental states and settings that either determines an application's behavior or in which an application event occurs and is interesting to the user."* reflects two different kinds of context that is *active* and *passive* context. This distinction helps to understand the use of context in mobile applications in that active context influences the behavior of applications whereas passive context does not. In particular, *active* means that applications automatically adapt to the discovered context by changing the application's behavior whereas *passive* means that an application present the new or updated context to an interested user or makes the context persistent for the user to retrieve it later. In dependence on the definition of *active* context-awareness we subscribe to the view of Chen et al. that this kind of context-awareness is likely to be more interesting for further investigations because it may possibly lead to new kinds of applications.

2.1.3 Definitions of Context

In order to understand what context is, how it can be used and how this knowledge helps to determine the context-aware behavior for particular applications we refer to definitions and categorizations of both, *context* and *context-awareness* as it is described by A. Dey et al. [27].

Their definition of context which is meanwhile generally known:

> "*Context is any information that can be used to characterize the situation of an entity. An entity is a person, place or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves.*."

By this definition, Dey et al. believe that it shall be easier for application developers to enumerate the context for certain application scenarios. They argue that context is information that can be used to characterize the situation of a participant in an interaction. A little example illustrates that by the use of two entities, the user and the applications, and two pieces of information, presence of other people and location, the location information can be used to characterize the user's situation and hence that the user's location is also context. We will later come back to the notion of location and discuss its importance in context-awareness.

Their elaboration on previous work on context distinguishes some definitions of context that, however, show that they are difficult to apply in practice. These definitions of context are closely related and basically refer to the same or at least similar combinations of context such as the location, identities of people and objects around the user, the time of the day, season, temperature. Also the emotional state of users, the user' environment and, in the same breath as location, also the orientation.

Other definitions of context A. Dey et al. refers to are rather synonyms for context. Examples include context as the user's or application's environment or elements of the user's environment that the user's computer knows about. The latter example was implemented by Brown [28] and is known as the *Stick-e-notes*. It was one of the first systems that considered context beyond location. But also situations such as the state of the application's surrounding todo: Ward et al. or the application's setting todo: Rodden et al. are accounted for context.

The combination of different context values such as location, entity, activity and time may further provide a better understanding of the current situation. Thus, if applications are able to process various kinds of different contexts retrieved from different sources it is possible that better conclusions can be drawn.

2.1.4 Early Examples of Context-Aware Applications

Chen and Kotz [26] enumerate briefly previous research in the field of context-awareness. What they write is basically an expansion of the work of Day and Abwod [27] (p. 9) who provide a table which shows different applications of context and an itemization of context-aware categories. Some of these systems are based on the *Active Badge System* [29] which was the first context-aware system that was scientifically investigated. It was designed and developed during 1989 and 1992 and later used as basis for the development of various other context-aware systems and applications.

Call Forwarding uses location information that is received with the help of the underlying *Active Badge System* to forward incoming calls.

Teleporting also termed "*follow me computing*" allows users to wander around while their location is being tracked by the *Active Badge* System. Based on the current location, the user interface is adapted according to the available resources.

Active Map is one of the earliest location-based services for indoor usage. It was developed by the Xerox PARC group and allows to locate each user with the help of wireless base stations that are mounted in each room.

Shopping Assistant is an application that aims to guide shoppers and help them in better finding and locating desired items, provide details of items and cost comparison between similar ones. The danger of violating the users' privacy is solved in so far as customers are distinguished by whether they are *regular customers* or *store customers*. Meanwhile, the latter case is realized long ago. The benefit of subscribed customers who receive discounts is balanced out by giving up their privacy.

Cyberguide [30, 31, 32] was developed at the Georgia Institute of Technology. Using the current user's location information received from a GPS receiver or in the indoor case with an infrared positioning system *Cyberguide* allows for dynamic interaction via an interactive map. Thus, leaving comments, finding right directions and receiving background information are the most noticeable features of the system. The ability to automatically collect and compile traces for the generation of a travel diary further allows the system to make suggestions based on previous patterns.

Conference Assistant was designed to support conferences and its participants. It uses the conference schedule as well as the conferences' attendance location information together with specific information regarding the presentation and information such as the research interests of the speaker. As a user enters a room, her name as well as additional information is displayed by the system to introduce the next talk.

People and Object Pager allows users to send nearby people message. If certain objects such as books in a library are requested, broadcast messages are sent out. Whenever someone encounters the requested book, she will be notified to pick it up for the requester.

Fieldwork is another early application that uses location and time information. The idea is to support fieldworker by providing means to ease the process of data collection. The collected data is further tagged with the current location information.

ComMotion from MIT [33] uses location and time to send reminder messages whenever a user enters or leaves certain pre-definded areas.

The examples listed here were published between 1992 and 2000. From todays' perspective, some of the used technologies seem to be outdated. Devices such as the Apple Newton[1] can be seen as the prime father of todays' mobile devices. Compared with todays' available technologies, these early systems form the cornerstones of devices and technologies that are available today and which basically provide only higher precision, resolution, processing power and communication abilities. However, the basic principles are still applied.

[1] Apple Newton technology overview: http://oldcomputers.net/apple-newton.html (last viewed 8. Aug. 2009)

2.1.5 Security and Privacy in Context-Aware Systems

There are a number of key problems such as ensuring the security and privacy in establishing secret communication and sharing personal information [20] which includes e.g. the difficulty of authenticating supplied location information from sensors. The growing number of users and the expected explosive distribution of devices that are connected to networks are the reason why privacy issues in context-aware systems are of keen interest and represent one of the most important research challenges. Since most people do not like the idea of being precisely located at any time, systems should provide means that allow users to be able to have the control over their contextual information in general which includes the accuracy of location information, who may access it and when to name only a few. As most research of modeling context is not limited to but focuses to a high degree on location information only [26] we can state without any doubt that the context plays a key design role for the development of distributed mobile applications. As already indicated, regarding context, location information represents probably the most important context variable.

2.1.6 Meaning and Importance of Location for Context-Aware Systems

Location information plays without any doubt an important role for the development of context-aware systems. Thereby, one important aspect is how a mobile device may determine the current position. Two general approaches to make a mobile device aware of its current location are discussed by Chen et al. [26] (p. 8):

1. The system tracks the location by monitoring beacons from mobile devices and the mobile device queries a central database to get the current location.

2. the mobile device passively listens to beacons from the cell base-station and queries a local database for its current location. In this case, if the mobile device only queries a local database for location, it has complete privacy and it can choose to advertise its current location to the world or only to selected third parties.

The latter one provides users with complete privacy towards third parties. An example application is the Privacy Observant Location System (POLS) that is referred in section 2.4.10 (p. 63). As already mentioned, the continuing emergence of new and enhanced technologies that allow for better localization of mobile devices and objects in combination with the emerging large-scale positioning systems discussed in section 2.2.5 (p. 19) pave the way for the realization of large-scale context-aware mobile applications as they were envisioned only a decade ago but could not be realized at these times due to the technological constraints. As a result the meaning and importance of location becomes evident in the light of context-aware systems.

So far the discussion about context allowed to identify *location* as to be one of the most important information sources with respect to *context-awareness*. The importance of location with respect to mobility leads directly to *location-awareness* (see section 2.2 (p. 13)). U. Leonhardt [34] continues his discussion about location by examining the relationship between *location-awareness* and *context-awareness*. Whereas *location-awareness* indeed does not necessarily lead to context-awareness, but, the other way round, *context-awareness* may be achieved even without *location-awareness*. Thus, even tough the importance of location

is evident with respect to mobility and *location-awareness*, it is not necessarily determining *context-awareness*.

Another interesting relationship between *location-awareness* and *context-awareness* is determined by the respective application at hand, or, in which context the notion of *location* is used. Whereas the intention and purpose of location-based services is usually determined by the desire to communicate and share location information or activities amongst users, in the light of social application awareness of location information includes more meaning than simply conveying someone's whereabouts. Especially in the certain case of families, knowledge about the location of each family member eclipses. Instead of telling the exact position, rather the affirmation of assumptions on things that are already known is in the foreground. Applications such as the *Whereabouts Clock* by [35] use location-awareness in this context which strengthens the emotional boundaries of families. In section 2.2.7 (p. 30) social services and applications are discussed in closer detail.

A way to explain location and context is to differentiate between different spaces and their interrelations. As such, mobile devices can exist in different spaces and hence have different locations. For example, a PDA is a physical device that exists only once in real space and has only one physical location. Almost any PDA provides a diversity of different means of communication such as WIFI, Bluetooth, GPRS, UMTS to name only a few. These devices can, to some extend, connect independently to a network or, once they are connected, switch to another network which provides better data throughput or quality of service. In essence, todays mobile devices can access remote services or and exchange information directly among each other.

Irrespective of the available network, the used protocols or any other technical means, the realization of mobile services that rely on location information from users that are part of and located in the physical world also provide some kind of digital representation of location information. The flow of information, in particular location information, from the real world to the virtual one and backwards is the key to many questions concerning context-awareness. The interrelation of different levels of representation of information, especially location information, is the starting basis for a number of questions in the field of mobile applications such as dynamic configuration, appropriate mapping of information in different levels, and of course questions concerning location security and privacy.

One important aspect in the discussion of location with respect to context is mobility. The consideration of location is especially of particular importance during the design phase of context-aware systems and applications. To be more concrete, location information has a considerable effect on objects, their behavior and interaction as well as communication. One extreme is a system that consists of only static objects. The relationships between these objects can be expressed merely as static configuration. The other extreme represents a solution that provides only mobile objects that communicate with each other. In this case, the necessity to frequently update each communication link, each state of the objects requires complex notification and representations models. In most cases application designers are confronted with a mix of both, static and mobile objects. In this case, even static objects are mobile in the sense that mobile objects may pass along. This changes the environmental state of static object and the communication. As many mobile objects pass along a static object, even the static objects require communication and adaption mechanisms that are similar to mobile objects. Thus, the differentiation between such objects must be based on other criteria.

Concerning mobility, Dix et al. [25] continues with a discussion and the development of a taxonomy of mobility. Their understanding of pervasiveness focuses especially on pervasive devices itself, the interrelations between pervasive devices and the *"expectation that these devices can work together to provide some form of shared functionality"* (p. 298) that is different from the general conception of pervasiveness as it is represented by Weiser [21] that devices disappear into the environment.

Their taxonomy provides two dimensions. The first distinguishes different levels of mobility which includes fixed, mobile and autonomous mobility. The second dimension considers the relation between devices such as *free*, *embedded* and *pervasive*. Finally, they investigate the nature of advanced applications together with the extend to which devices are bound to individuals or groups which is reflected by *personal*, *group* or *public*.

The explanations in this section show the importance of location for context-aware systems. The following section narrows down from the very general notion of context-awareness to location-based services which certainly rely on many different key technologies and methodologies as we have briefly discussed some of them so far.

2.2 Location-Based Services

Probably one of the most frequently asked questions of mobile users at the start or during conversation is *"Where are you?"*. It is an evidence that location is an element of uncertainty in mobile communications [36] (p. 94). This, toghether with the mobile network operators ability to determine the current position of each connected mobile user suggests the development of mobile services and applications that provide, share and process the actual location of mobile users [37] also referred to as *Location-Based Services* (LBS) and discussed in closer detail in this section.

The opposite to this uncertainty can be referred to as *location-awareness* which, as discussed by Leonhardt [34] is the result of mobility of mobile phones that have the ability to interact. This interaction is only possible when the phone is within the range of a base station. Thus, in order to be able to provide services, the actual location and knowledge of it is essential and leads to the requirement of location-awareness.

This awareness is certainly an important prerequisite for the development of location-based services but at the same time the question where someone or something actually is does certainly not represent an location-based service per se nor hold for a definition thereof. The answer to this question is much more complex than simply stating that the retrieval of location information is directly related to the corresponding location of some user [38].

In [39] Wu and Sun cite E. McCabe idendify four factors that are driving the development of location service systems. This includes *accuracy of positioning technologies*, *integration of wireless communication mechanisms*, *establishment of industrial standards* and the *development of INs (Intelligent Networks)*. The explanations on location-based services in this dissertation can be referred to each of these factor throughout. But first of all we give an overview and at the same time an in depth analysis of what constitutes the various existing different kinds of location-based services. Therefore, we start with an illustration of the very complex and evolving matter of location-based services by means of a collection of definitions and statements that in our understanding describes the issue very well.

2.2.1 Definitions and Interpretations

ISO[2] defines the notion of location as *"identifiable geographic place re-presented by any one of a set of data types that describe a position, along with metadata about that data. A location is represented by one of a set of data types that describe a position, along with metadata about that data, including coordinates (from a coordinate reference system), a measure (from a linear referencing system), or an address (from an address system)"*. ISO[3] defines location-based services as *"Service whose return or other property is dependent on the location of the client requesting the service or of some other thing, object or person"*.

As there are exist various definitions of location-based services and each of them does not provide a complete answer to all questions, also the following discussion can only cover a small subset of the whole issue and thus represent a representative cross section instead. We start with a very brief definition by Junglas et al. [40] who stat that *"Location Based Services (LBS) are services that take into account the geographic location of a user"*. In contrast to that Adusei et al. [41] (p. 1) are bit more specific: *"Location Based Services are business and customer services that give users a set of services starting from the geographic location of the client"*. Both definitions seem to provide a very specific explanation what location-based services are. However, as the following definition shows, the problem cannot be tackled so easy as it seems.

As Küpper [42] (p. 1) alludes there is no common definition or terminology for the term *location-based service*. Confusingly, the term *location-based service* itself is often used interchangeably with *location-aware service*, *location-realted service* or *location service*. Since there seems to be no absolute answer to the question what location-based services are, the aim of the rest of this section is to provide at least the most general ideas and, what is even more important, to prepare for an in depth evaluation of the proposed solution.

2.2.2 Background on Location-Based Services

Technically, Location-Based Services comprise a number of different technologies that can be classified into the three basic categories as follows[41]:

- *Services*: This represents products (commercial and free) that are available to customers. This includes a variety of most diverse products. Systems, services and applications for all kinds of navigation systems, new kinds of social applications and emergency applications are only a few examples of what is offered as services in this area today. section 2.2.7 p. 27 gives an overview about different kinds of location-based applications.

- *Features*: include the very important but still often underestimated issue of user interfaces and usability in accordance with security and privacy checking. This has certainly an impact on personalization and charging and thus consequences not only on the client side but also on the back-end systems and services.

[2]ISO 19112:2003 Geographic information Spatial referencing by geographic identifiers
[3]ISO 19133:2005 Geographic information Location-based services Tracking and Navigation

- *Enablers*: or *enabling* location technologies refer to the basic technologies that are necessary to obtain the location of a mobile user. Localization is a basic function in mobile networks and without it the operation of mobile networks would be impossible. So, operators have to provide additional features and deliver services that allow access to customers' location information in a secure an privacy protecting manner. In the next section 2.2.3 p. 16 we discuss the basic functions that are necessary for the operation of mobile networks in terms of localization.

In [38] Dibdin lists some enabling technologies such as Cell-ID, Round Trip Time, Observed Time Difference, Satellite and Assisted GPS. We discuss each of them in detail below. On the contrary, *facilitating* technologies refer to technologies that are used for the contextual and infrastructural environment *"within which MLS can be implemented in a value added fashion"* Giaglis et al. [43] (p. 69).[4] Giaglis further distinguishes enabling technologies into *mobile network-dependent* technologies and *mobile network-independent* technologies which are both discussed later in this section.

About a decade ago the advent of location-based services promised to be the next killer application on the mobile market. As a result at the early stages of the location-based services development, most of the market estimations were exaggerated or wrong. Maybe these misconceptions and misinterpretations are the reason why even today the whole location-based service area is still viewed as problematic, in spite of the fact that today a multitude of location-based services is available on the market. Thus, the argumentation that the promised take-off seems to have failed to appear is simply wrong. In fact, the location-based market meanwhile provides a noticable variety of solutions and is even deemed to be one of the biggest growth sectors[5]. Most of the commercially available navigation systems are developed by hardware manufacturers. In a meanwhile rapidly growing market there seems to be not much space left for the manufacturers to take into consideration the vivid scientific experience and input that already exists in this field. Raper et al. [20] (p. 17) continues with a comparison of different research activities that are undertaken in the light of *wayfinding* on mobile devices. In this context, it turns out that the directions given by in-car navigation systems are researched at best. As a result of the scientific research in this field is that there is a noticeable dissatisfaction related to the adequacy of the directions. One reason for that are poorly designed instructions and the chosen routes. But there is also an evidently need for novel user interfaces that reduce the cognitive load of the driver and make this kind of applications more complaisant to the user.

The next wave of high expectations in the location-based market is steamed up by *Global Navigation Satellite Systems* (GNSS), a generic sense that brings in to line different individual systems like the prestigious European *Galileo* project, the Russian *GLONASS*, the already long running American global positioning system *GPS*, Japans Quasi Zenith Satellite System *QZSS*[6] and satellite based augmentation system *SBAS*. This includes also regional systems such as the Indian Regional Navigational Satellite System (IRNS)[7][8] as well as other

[4] Giaglis refers to *Mobile Location Services* (MLS)

[5] URL: http://www.tagesschau.de/multimedia/video/video239272.html (last viewed 27. Nov. 2007)

[6] URL: http://www.jaxa.jp/projects/sat/qzss/index_e.html (last viewed 10. Oct. 2008)

[7] URL: http://www.rediff.com/news/2007/sep/27gps.htm (last viewed 27. Sep. 2007)

[8] URL: http://www.livemint.com/2007/09/05002237/India-to-build-a-constellation.html (last viewed 5. Sep. 2007)

systems that will emerge in future. It is obvious, that especially since 24.11.2007 when the European Union ensured the financing of Galileo also research in this field will gain strong momentum. This explains why especially during the last years the improvements of positioning techniques, data transfer rates for mobile devices increased by the use of UMTS and the manufacturers that put enormous efforts into the miniaturization and enhancements of mobile devices and sensor technology will not only be continued but will be further fostered by the recent developments and expectations in the emerging location-based markets.

This development shows a clear trend towards standardized solutions. It shows, that the many possible future location-based systems that are developed in the near future for and with the use of e.g. the Galileo System[9] depend not only on local but global technical and standardization agreements. Past examples from the mobile industry show, that it is difficult to set up and accomplish worldwide standards. The same may happen to the global navigation systems. Although Galileo is designed such that different localization technologies can be used, it still remains open how the technical realization will actually look like.

It is foreseeable that in the near future the mobile industry may become an important part of the global navigation systems. By now, almost any new mobile device provides a GPS receiver. With the emergence of the first commercially available Galileo receivers, especially in Europe the mobile industry will adapt this technology and integrate it into their products. It remains to be seen what kind of new applications will be available that utilize the various possible new services and how network operators integrate these services into their existing landscape. One important question is if this development solves the problem that is currently termed as *"paradox of mobile location services"*. It reflects the current situation where services are per definition local but in an increasing degree required globally. Service portability, roaming and other technical issues to the point of billing have to be solved on a global scale. In section 4.7 p. 125 we propose a solution that overcomes many of currently existing obstacles.

2.2.3 Operations related to Localizations in GSM Networks

Knowledge about the current location of mobile users is vital for the operation of mobile networks. In the following we will discuss the basic functions and operations that are necessary to establish phone or data connections to mobile devices.

Basically, there are two types of functions that are in use to determine the location of mobile stations. One is the so called *Location Update* (LU) the second one is called *paging*. Whereas in case of LU the Mobile Equipment (ME) communicates its own position to the network, *paging* works the other way round in that the network looks for the ME and thereby learns its actual position.

There are two possible reasons for inducing a LU: First, the LU is issued periodically independent of whether a new *Location Area* (LA) was entered or not. We will discuss location areas later. The advantage of this strategy is that even though no new location area was entered (which forces the execution of the LU) and no phone call took place, the network is still informed about the current location which e.g. eases restoring errors in databases in case of failures.

[9] Galileo Application's Day (2. May 2007) URL: http://www.ffg.at/content.php?cid=318&sid=89

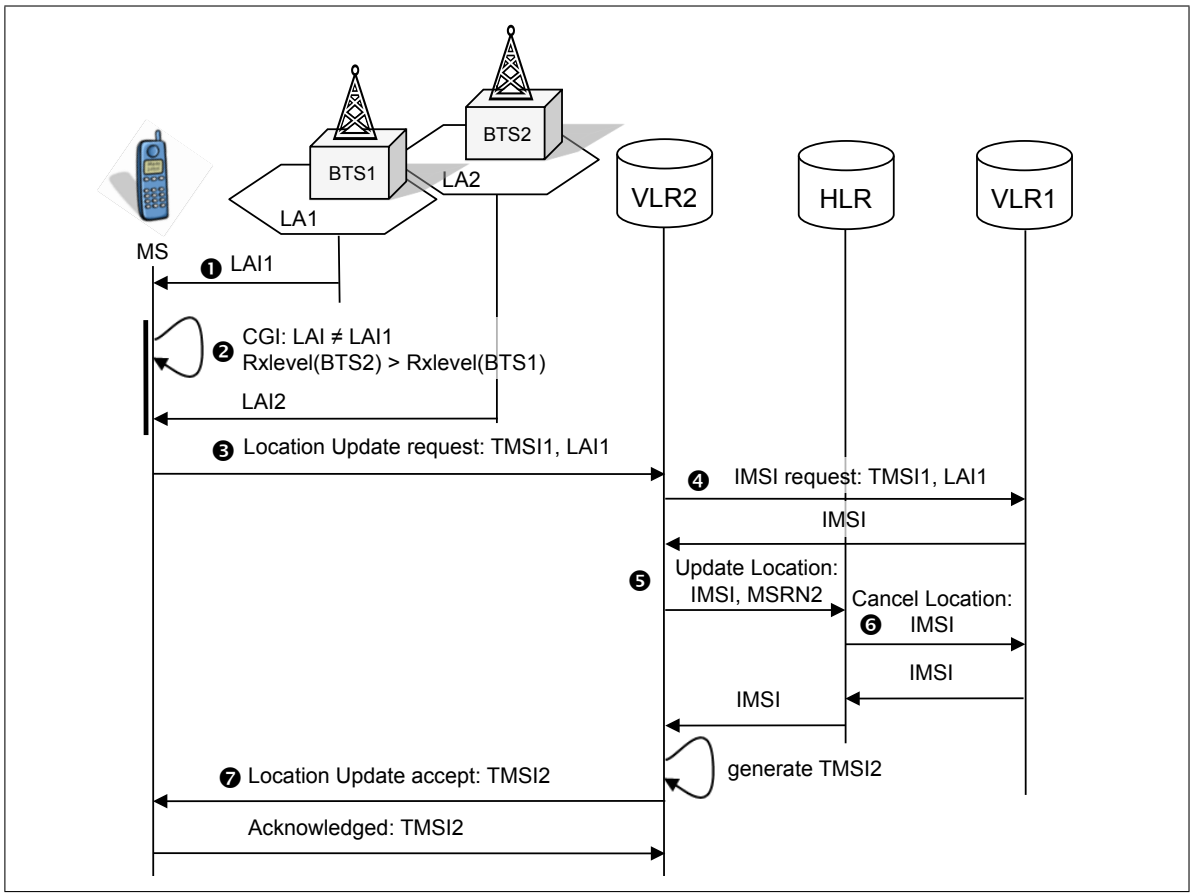

Figure 2.1: Location Update in the GSM Network [1]

The second reason for a LU was just mentioned and is the change from one LA to another. Several Base Stations (BS) or short *cells* may be combined to a LA which is identified by the *Location Area Identity* (LAI) and may be controlled by the same *Base Station Controller* (BSC). If one LA contains two or more BSCs, they have to be served by the same *Mobile Switching Centre* (MSC). The number of cells that are part of a LA is up to the design of the network operator and depends on the given local conditions.

Location Update Operations

Figure 2.1 [42] (p. 109) depicts the two possible reasons for the initiation of a LU. One is that the mobile device enters a different Location Area. While the mobile device moves, it controls the signal strength of all the neighboring base stations it can receive. At a certain point the signal of another cell may be stronger than the one the mobile is currently connected to. This forces the mobile device to switch to that other BS. Each cell broadcasts its LAI on a dedicated broadcast channel. The last received LAI is also stored on the *Subscriber Identity Module* (SIM) . If the received LAI differs from the stored LAI on the SIM, the mobile has to induce a LU. This also happens if the SIM is inserted and activated.

In figure 2.1 message 1 shows the LAI transmitted to the MS via the broadcast channel. Message 2 shows the possible case that the received LAI differs from the one that is stored on the MS's SIM. Second, the observed signal level of BTS2 is stronger than that of BTS2. Additionally, this BTS2 is part LA2 which also causes the MS to force a LU. Message 3- prepresents the actual *Location Update Request*. It contains as parameters the *Temporary Mobile Subscriber Identifier* (TMSI) and the LAI currently stored on the SIM. Since the TMSI is only a temporary identity which is generated and assigned by the VLR for security reasons, VLR2 which is now responsible for the ME asks VLR1 for the *International Mobile Subscriber Identity* (IMSI). This is used for network internal purposes only such as international roaming, account of charges and as network internal addressing for the *Home Location Register* (HLR).

Next, the mobile authenticates itself and the new LA is registered in the VLR of the MSC in charge. If the MSC has no user information available, it is first loaded from the HLR, then the location of the user can be registered at the VLR. Finally, the user's data is updated at the HLR. This update includes the new LA and possibly the new address of the VLR [44] (p. 260).

In case no active voice call or data is transmitted, the only available location information is the LA. The network may send a *Silent SMS* which induces the mobile to react. By this means the location information of a mobile can be requested for the purpose of e.g. location-based services. This *Paging* process was already mentioned in the beginning of this section and can be used to determine the location of a mobile as it is described in the prototype description in section 4.3.2 (p. 106).

As already indicated, the location information that is generated and stored by the network operator may not only serve for the establishment of voice calls and the operation of the network. It is also value information that can be used for the realization of different kinds of location-based applications. Since operators are even obliged to provide precise location information, the processing and protection of location information plays an important role especially in the light of location-based services and applications. section 2.2.7 (27) provides a detailed discussion with regard to different forms of location-based applications.

Another network intrinsic procedure is the so called *handover* which is initiated only during active voice calls or data transmission. There are certain different possible kinds of handover such as quality handover, handover caused by congestion, velocity based handover and service based handover. A handover may also induce a *Location Update* (LU).

After this short discussion about some basic principles and facts about location-based services and a description of some of the fundamental network operator's principles regarding the mobile's location and the determination thereof, in the following we continue with a short comparison between location-based services and context-aware computing which was described at the beginning.

2.2.4 Comparison between Location-Based Services and Context-Aware Computing

This section discusses location-based services that are a subset of the more general context-aware services was we have already discussed in the previous section about context 2.1 p. 5 and by Küpper [42] (p. 2). Location-based services mainly imply the processing of location

data as the most prominent context information beside time, temperature, pressure, light intensity or any kind of radiation but also information that includes the human factor such as information about someones identity or activity to name only a few. Location-based services basically rely on the the most prominent context variable that is location information. This can be expressed in different ways such as e.g. geographic coordinates or abstract descriptions. The specificity of location-based services aims for the processing of location information independent from the actual representation. Therefore, it provides functions such as those for filtering, selection, discard and conveying of location information but may also include the processing of other interrelated context information as well. In this regard Küpper [42] distinguishes further between location-based services which only perform high-level actions and the so called *location service* which generates and provides the location information to the location-based service. These two services mostly appear in conjunction. If there is no location service available, the location information has to be entered by the user.

After this brief comparison between *Context-Aware Computing* and *Location-Based Services* we continue this discussion with an in depth analysis of these two similar but anyhow in some respects distinct concepts and show the commonalities as well as the differences. Additional examples will demonstrate the applicability of these concepts from a practical point of view. One purpose of this discussion is also to prepare the reader for a better understanding of the whole matter and as a prearrangement for the own presented solution.

2.2.5 Location Technologies

Over decades different location technologies have been developed and improved. The specific characteristics of these technologies affect various factors such as precision and accuracy of the location information. In order to understand certain characteristics of location-based services a solid classification of the underlying location technologies is an essential precondition for the development of location-based applications.

Duckham et al. [45] assert two different classes of positioning systems, that are *active* and *passive* positioning systems. *Active* systems rely on beacons and include WiFi, GPS, bluetooth or infrared. These are the most popular ones. On the contrary, *passive* systems such as *inertial navigation systems* require no beacon. They solely rely on sensors that continually track the position, orientation and velocity of the mobile device. The currently available 3G[10] mobile devices such the iPhone[11] or the Nokia N95[12] are meanwhile by default equipped with a variety of sensors and allow the implementation of interesting applications that make use of these sensors [46].

According to B. Schilit et al. [47], *passive* systems can further be distinguished into three localization types that are either *network-based*, *network-assisted* or *client-based*. This scheme gives information with regard to privacy preserving aspects and also corresponds to the different business scenarios in the mobile business (see section 2.3.3 (p. 42)).

[10] 3G stands for 3^{rd} generation and is used as an abbreviation for Universal Mobile Telecommunications System (UMTS)

[11] iPhone URL: http://www.apple.com/iphone/ (last visited 8. Aug. 2009)

[12] Nokia N95 URL: http://europe.nokia.com/find-products/nseries (last visited 8. Aug. 2009)

Three types of localization:

- *network-based* positioning systems: in this scenario the location of the mobile devices is solely determined by the network operator. This is usually done with the help of the cell-ID which is generated and used exclusively by the network operator.

- *network-assisted* positioning systems: the combination of client-based and network-based positioning allows better determination of the current location. Technologies such as A-GPS (Assisted GPS) make use of both, the network operators cell-ID and the GPS information received by the client.

- *client-based* positioning systems: navigation systems are a representative example for this category of positioning systems. Devices applied with sensors are supportive in addition to built in GPS receivers. This allows not only the development of applications that include the current position but also the orientation, pitch or acceleration of the mobile. This kind is also referred as *user-centric* approach (A. Küpper and G. Treu [37] p. 5) and, as they show, reflects the Web 2.0 concept. An overview about possible future developments that follow this approach is given in section 2.2.10 (p. 37).

The following three subsections provide a concise overview of some of the most important localization technologies that are in use today. As already stated at the beginning of this section, this includes *mobile network-dependent* and *mobile network-independent* technologies as a specialization of the so called *enabling technologies* [43] (p. 69) as well as various combinations of different localization technologies.

Mobile Network-Dependent Technologies

- *Cell-based Position Determination*: The GSM network determines the cell of the mobile station in which the mobile is currently booked. The coordinates of the base station or a characteristic coordinate of the cell.

  When a mobile device connects to a mobile network, the Mobile Services Switching Center (MSC) which serves the Base Station the mobile device is connected to, synchronizes the location information with the HLR which is the central point for administration and the Visitor Location Register that is maintained by the MSC. The mobile network relies on the location information administered by these databases for the establishment and termination of connections. Thus, location information plays a viable prerequisite for the operation of the mobile network.

  But, *cell-based* positioning technologies deliver only the approximate position of the device since the accuracy of this kind of positioning technology is limited to and covers only the cell size which varies depending on the mobile network design. Whereas in urban areas the precision may be up to 100m, in the countryside the range of one cell may be as large as 40km.

  In urban areas the density of antennas is mostly high enough and thus the current location information of a mobile device is usually precise enough to serve a wide range of location-based applications. But, as soon as the mobile device moves to the countryside,

the distribution of antennas is characterised by far distances which may render location-based applications in some cases rather useless.

Compared to GPS localizations (see below) which requires line-of-sight to satellites, this technology allows localisations of users even if they are in buildings or in the underground. However, one decisive disadvantage is that the accuracy of the location may be not sufficiently high enough for certain applications. Whereas the density of antennas in urban areas is mostly high enough to provide location data with sufficient precision, in the countryside the distribution of antennas is characterised by far distances which may render location-based applications rather useless.

- GSM fingerprinting is a localization method that allows to use the existing network operators infrastructure, that is in particular the cellular base stations. This technology can is not only applicable for outdoor localization. Otsason [48] shows that it is also possible to use GSM fingerprinting for fine-grained indoor localizations that differentiate between floors of wooden or steal-reinforced concrete buildings.

- Time of Arrival (TOA) This method uses is based on the time the signal needs from one communication point to another. The signal is sent to three different cells and the signal propagation delay is measured and compared. This method is also known as *tirangulation*. With this method high accuracy can be achieved. But, each cell additionally has to be equipped with so called *Location Measurement Units* LMUs which are synchronized with the GPS. Upgrading the network with LMUs also means that network operators have to invest an considerable amount of money.

- Observed Time Difference (OTD) The OTD method is quite similar to the TDOA. In this case additional costs can partly be passed on to the customers. In comparison to TDOA the OTD requires mobile devices that are enabled to perform the triangulation. This significantly reduces the required number of LMUs such that only a minimum number of LMUs are required.

- Assisted GPS (AGPS): As the name suggests, in this specific case the network operator or a service provider assists the mobile devices in the process of determining the location. This is of special importance in case the mobile device does not dispose of good signal. This may have different reasons such as shielding or in case of indoor localizations. Another reason why AGPS is beneficial over GPS or Cell-based localization is strongly related to the so called *Time To First Fix* TTFF which expresses the time that is needed until the receiver has calculated the first so called "*fix*". In case of AGPS where the mobile device is supported the time needed to determine the location as well as the power consumption of the mobile device can be reduced by enhancing the accuracy of the calculated position. The so called "*cold start*" which can last up to several minutes can be reduced significantly.

  Different methods can be applied to determine the mobile device's location such as directing the mobile device to either look for dedicated satellites, or by carrying out computational intensive calculations on behalf of the mobile device. This may include the information at which of the network operator's cells the mobile phone is currently

connected to and mixing this information with possibly only rough data received so far by mobile device from satellites.

The support of such dedicated servers allows to reduce the TTFF and localizations with very high precisions up to 2-3 meters [49].

K. Kyamakya discusses in [50] network dependent technologies and shows synergy effects and their benefits for customers in terms of cost benefits expressed as an estimation of the ROI (Return On Investment).

Mobile Network-Independent Technologies

- *GPS* is meanwhile one of the most important application technologies many applications such as in-car navigation (see 2.2.7 p. 27) rely on. Basically, GPS comprises three segments, the *space segment*, *control segment* and the *user segment* [51] (p. 2).

  In the *space segment* nominally 24 satellites circuit on six different orbits around the globe. The *control segement* consists of five stations located in Colorado Springs, Hawaii, Acension Island, Diego Garcia and Kwajalein. The stations are arranged all over the globe in such a way that the connectivity and control of each satellite is at 92%.

  The *control segment* monitors and controls the *space segment*. Each station is equipped with a GPS receiver. The Colorado Springs station is the central point where the information received from the other stations is collected and analyzed. This includes also synchronization of each stations watch that has to be synchronized with the satellites atom clocks. Equally, the central station induces corrections to the satellites steering to orbit a satellite if necessary.

  The third one is the *user segment* which represents the total of all GPS receivers. It comprises a number of different GPS receiver technologies. Apart from the GPS receivers that are sold on the mass market there are also receivers that are used for dedicated purposes such as navigation and survey applications only. Some of the most important navigation satellite systems were already mentioned in section 2.2.2 (p. 14).

- *Bluetooth* IEEE 802.15.1 [52], is a specification for short-range radios used for point-to-multipoint data transfer. The range is between approximately 10 centimeters to 100 meters. With higher transmission power it is also possible to reach 100 meters. Bluetooth was initially developed for the realization of ad-hoc connection between different kinds stationary and mobile devices. Beyond that it can be used to identify the actual location of a device [53]. In comparison to other localization technologies this one provides very high accuracy since each Bluetooth range is very small.

- *Wireless Fidelity* short WIFI resembles the mobile network infrastructure. In both cases mobile devices communicate with base stations. Especially in cities the density of WIFIs is in some places even very high and thus allows WIFI fingerprinting. This requires an initial phase where for dedicated places the signal patterns of the surrounding WIFI stations are received and stored together with the measured exact position (usually GPS). This association is then transferred to and stored by a database. Subsequently, the actual position can be queried either by sending the measured pattern to the database

where the associated location is stored (terminal-supported). In case of the terminal-based mode both, measurement and evaluation of the respective location information is calculated on the mobile device. Finally, for the network-based approach access points receive a list of beacons from the terminal whereupon a central server calculates the signal strength for the calculation of the position.

- Visual-based Localization: P. Pace et al. [54] distinguishes two possible systems. One system uses the pictures of the environment as source and analyzes this with some pictures that were captured earlier. The second one uses markers that have to be placed in the environment. They state that both of these technologies have advantages and disadvantages. First, visual-based localization can be applied to both, outdoor and indoor localization. Second, this kind of system does not need any beacons. A drawback of such a technology is that if the environment changes, the system might not be able to identify the reference objects and hence is unable to determine the location.

Mixed and Other Technologies

Location determination techniques such as *dead reckoning* are simple and used for a long time. It is a process where the position of an object is estimated upon some previous position or fix by inclusion of the current speed, elapsed time and the course. This technique goes back to the ancient chinese times when they discovered that a needle with a magnet always points towards north. With this information and by multiplying their speed by the time spent by traveling, they were able to deduce their current position[13].

This technique was also used in Europe e.g. at the time of Christopher Columbus' rediscoveries of the new world till the accomplishment of the marine chronometer. Dead Reckoning was also used for aviation navigation. Today this kind of location determination is used still used, mostly in combination with GPS, WiFi, or RFID to namely only a few.

Another localization technique that provides even higher accuracy than the network can is based on the combination of the current *Cell-id* and a location database that contains associations between different location information sources such as the cell-id and precise location information such as GPS locations. This technique requires some preparatory work which is called *geo-referencing* which for example documents each change-over from one cell to another and assign this with precise location information that is received from a GPS receiver. The more such change-overs are registered, the more precise the following localizations are. This kind of localization as well as its operation in a large scale application is documented in [55].

As already indicated, the use of GPS location information is beneficial in many ways. Beside some disadvantages observed in some urban areas where not enough satellite links GPS can be provided due to concrete canyons, GPS provides location information with high precision. As a consequence, todays location-based systems make increased use of the GPS. Even network operators offer navigation solutions that solely rely on location information that is received by the mobile[14]. In comparison to systems that use location data that is generated and processed by the network operator, this location information cannot be added

[13]URL: http://www.deadreckoning.com/ (last visited 27. Feb. 2009)

[14]network operators navigation solution: http://www.a1.net/privat/navi (last visited 27. Feb. 2009)

to the notion of *location data* as it is defined in the European Union. The reason for that is that GPS data is not necessary to establish a communication.

At the first glance this differentiation seems to be a bit pedantic. However, there are cases when the consent of a user to process and forward the own location information is required. The European Directive EU 2002/58/EC [13] expresses this in article 9 by:

> *"The service provider must inform the users or subscriber, prior to obtaining their consent, of the type of location dat which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service".*

2.2.6 Classification of Location-Based Services

Position-aware and Location-Tracking Applications: Junglas et al. [40] and Barkhuus et al. [56] discuss possible classifications of location-based services distinguish two classes that are generally named *position-aware* and *location-tracking services*. These two kinds of services can be identified and distinguished basically by the role of the requester and the recipient of the requested information.

In position-based services which are also often referred to as *location-aware services* information is received by the user who is at the same time the requester. Therefore, requester may provide their actual location information in order to receive location-dependent information. One example for is the shortest route to some point of interest.

In contrast to that, *location-tracking services* receive requests from and provide location information to external third-party applications which act on behalf of the users. In this case, the requester and the receiver are not necessarily the same.

As mentioned above, location-tracking applications differ from position-aware applications in that the service requester does not necessarily have to be the same person. This allows to request services that collect and process position information on behalf of the requester not only for a single but even many persons or objects at once. Another distinction is that position-aware applications respond to each single service request whereas location-tracking applications' processes are activated once to collect and process location information of several users. This possibly includes the requesters' location information.

Reactive and Proactive Location-Based Services: Another possible way of classification is to distinguish whether a location-based service is *reactive* or *proactive* [57]. Wherease reactive location-based services only deliver location information upon the users' request proactive services operate on sessions and react on predefined events. According to Bellavista et al. [58] reactive and proactive services are closely related to position-aware and location-tracking applications.

For example, for reactive location-based services user may usually request for some information that is tightly coupled with the current position of the user. This refers to position-aware applications which deliver information of e.g. nearby points of interests. In this case, the requester is the same person as the receiver of the information. For the sake of clarity, it is not so important how the location information was received.

Either the user provides the location information by herself as part of the request, or the location is determined by other means than the user e.g. by the network operator.

Whereas reactive location-based services rely on users interaction, proactive applications can operate more autonomously. Once they are started they detect and react location changes, trigger certain actions change states. The possible interaction patterns are manyfold and usually based on proximity detection of users or other target objects.

The decisive distinction between reactive and proactive services is that reactive services provide users only a synchronous communication pattern whereas proactive services allow users to communicate asynchronously. Another distinction that goes along with the discussion of synchronous and asynchronous message patterns is that of sessions. Whereas asynchronous communication requires in any case some means of session management, synchronous interactions do not necessarily require the establishment and management at least of long term sessions. Usually, each request is processed in form of a blocking call. Sessions that were established for that purpose are immediately torn down as the called function returns the result.

According to the synchronous communication pattern reactive service applications basically require only some location information to generate added value. One popular example represents the meanwhile widespread use of car navigation systems that processes the cars' actual position information that is received from the satellite. The location information is processed directly on the navigation device and for example instantly displayed on as a map on the screen. Todays navigation systems further allow processing of various kinds of additional information such as for travel planning, congestion detection, radar warning to mention only a few. Most of these additional functions require remote information that is accessed by means of wireless communication. The basic functionality of car navigation systems, that is the internal processing of received GPS position information demonstrates a typical example of position-aware services. Due to the extended communication capabilities of nowadays mobile devices, this kind of navigation systems can also be added on to the type of sporadic queries which is discussed in the following.

Location-of-target and Target-at-location: Whereas most location-based services are designed to first collect and process location information about persons or objects and then use this information possibly in combination with other information sources, Weiß et al. [59] refer to a different class of location-based services which is called *Zone Services*. Here, a location or geographical zone is given as starting point for e.g. the determination of the numbers of users or objects that are currently within the vicinity.

In [37] (p. 10) A. Küpper and G. Treu similarly distinguish these two possible kinds of mappings and denominate those location-based services that follow the traditional mapping that is from users or in general objects to the location as *location-of-target* whereas the determination of the number or even the identities of those users that are currently within the vicinity of another object or in a certain area are referred as *target-at-locatoin*.

Sporadic Queries: Another classification is proposed by Gruteser et al. [60]. In addition to the already discussed classification of location-based services that distinguishes between position-aware and location-tracking services they provide an additional criteria that is *sporadic queries*. This subsumes all services that allow users to initiate the transfer of location information to an outside service provider. Gruteser carry on that such queries contain only the current user's location- position information.

Self and Cross Referencing Location-Based Services: The question who the requester is and who receives the particular answer was already identified as a distinctive feature of position-aware and location-tracking applications. Similarly, the question whether an application can be added to self and cross referencing application is closely related to that of who the requester and the receiver are.

As a result, cross-referencing location-based services require more stronger means of users privacy protection and should be restricted to access location information of only well defined groups of users that gave their explicit consent [58]

Single and Multi-target: The actual number of users being part of an active session allows to distinguish between single and multi-target location-based services. It is clear that this also location-based services that are capable of tracking multiple users or objects at once may can also be subsumed to the single-target location-based services. A distinction that makes probably more sense is given by Bellavista et al. [58]. They count applications those applications to the single tracking ones that track only one target. Simple scenarios as these may for example have only one implemented functionality such as displaying the actual location of the user being tracked on a map. On the other hand, the focus of multi-target applications is rather on interrelating positions of several users that are tracked in one or possibly several sessions.

Content- and Application-orientation: The kind of information that is exchanged allows for another classification that is whether a locatin-based application is content or application oriented. In the case of content oriented applications usually location-dependent information is exchanged. There are meanwhile many examples for location-dependen content delivered to users.

In contrast to content orientation, application oriented means location dependent discovery, download, installation and deinstallation of applications and application components without any additional user interaction being required. Compared to mobile applications that are requested by the users, location-based services that are also application oriented introduce a number of challenges as they occur with such complex interaction models and of course the resulting security and privacy requirement.

Outdoor and Indoor: There are a number of localization technologies that can only be used for outdoor positioning while others are rather better suited to be used indoor. As opposed to outdoor technologies, for indoor localization more efforts such as calibration, learning phases are required. cite ?

2.2.7 Examples of Location-Based Applications

The list of currently available and technically possible localization technologies suggests that the list of available location-based applications is much greater. Thus, it is impossible to present not even a subset.

But, even though it is to provide a clear and concise definition of what a location-based service or application actually is, with the help of the used localization type, the communication and interaction patterns and dedicated knowledge about the area for which the applications are developed, it is possible to conduct proper classifications for each new application. One such widely used classification scheme is proposed by Giaglis et al. [43] (p. 66).

Emergency Services

The network operators obligation to provide means that allow to locate people in an emergency was the starting point for further technological refinement and since then fostered the development of various kinds of location-based services and applications. Meanwhile the spectrum of support systems for *emergency support for vehicles* is fairly broad [61]. One prominent example in this respect is that of passengers of vehicles in an emergency case that is caused by an accident or motor vehicle losses. Especially in case of an accident when the casualties are not aware of their position or even not able to communicate at all because of lost consciousness the possibility to determine the position can even safe lives. One problem in this regard is how the device or system can detect emergency cases without user intervention? With the help of sensors for impact detection the vehicle itself could send out emergency calls or use the mobile phones communication capabilities.

Another class of emergency services provides users the ability to deliberately send emergency calls such as in the case of an accident or almost any kind of thread. One example which is not bound to the use of mobile phones but all the more relies on the ability to detect the exact location is the avalanche transceiver[15] or a system that uses reflectors as passive locating devices which are sew into almost any garment or available as sticker[16].

As stated in the introductory part of this section, the analysis of movement patterns reveals much about human trajectories. This knowledge can be used for the development of new and even more precise models that provide higher accuracy on forecasting mobile viruses. As a result, this enables better epidemic prevention and emergency response procedures which can safe lives.

In the paper titled *Context-Aware Emergency Coordination Systems* [62] Kurschl et al. raise the question of how to define and model applications that support emergency scenarios. They state that at the moment research on context information focuses on sensor technology and how to best utilize this through the aggregation and interpretation of the available context information.

Navigation Services

The next group of location-based services can be labeled as *navigation services*. Examples for such services and applications can be related to any of the already discussed classification

[15] Avalance tranceivers: http://en.wikipedia.org/wiki/Avalanche_transceiver (last visited 17. Feb. 2009)
[16] RECCO: http://en.wikipedia.org/wiki/RECCO (last visited 17. Feb. 2009)

category. This includes various applications such as e.g. show users their actual position on a map and draw a route to the desired destination. Web applications that allow users to calculate routes are available for a fairly long time. Mainly due to the advent of mobile devices navigation services have latterly gained significant popularity. In the foreseeable future, navigation services are expected to be part of almost every mobile device.

Navigation systems and services on the web include Google Maps[17] and ViaMichelin[18] to name only a few. Aside from navigation services that are specialized for in-car or bike navigation like TomTom[19] which mainly rely on GPS as location source, also specialized solutions that make use of Wifi networks to determine the location are available. One such example is currently deployed on mobile devices such as the iPhone and iPod touch[20]. Another way to determine the current location of the mobile device by using the software LocateMe[21] that is provided by Sonerois, a developer for games and applications for the iPhone. This software primarily uses the available cell information from the network operator but also other sources that are not clearly specified. Software like this raises a set of legal problems which are explained and discussed in detail in section 2.4.2 (p. 52).

As a consequence the question arises is if such software can from case to case be counted to so called *Disruptive Innovations*. Similarly, *Disruptive Technologies* can be described as to be cheaper, simpler, smaller and more convenient to use [63] (p. 9), [64] (p. 41).

Osterwalder et al. [65] discuss such innovations regarding a comparison between the business model of Skype and those of a frictional Telco. The question is, do applications like LocateMe or nav4all or even the entire area of free available software contain enough disruptive potential to be classified as disruptive innovation? And if so, what are the consequences in the location-based service area? Is it possible that existing professional location-based services are threatened by such applications and what about location-based services offered by Telcos? Is there a likelihood that such applications have an impact on the telecom market? And if, what about other branches of industry? For example, one might think that professional applications such as those that are used for e.g. container shipping [66] do most likely not tangent such disruptive innovations. The reason is that such critical and widely ramified applications rely on sensitive data and many other systems that are mostly not publicity available. Anyhow, as one would think that this applies to almost any technology or branch of industry the delineated examples show quite the opposite. Furthermore, innovative and easy to use technologies such as Fire Eagle [22] are predestinated to use location information in an easy way. As industry is constantly looking forward to better utilize their resources it is no surprise that some new prototypes and applications for internal use are e.g. *Mashups* and *Web 2.0* technologies in general.

[17] URL: http://maps.google.com (last visited 14. Feb. 2009)
[18] URL: http://www.viamichelin.com (last visited 14. Feb. 2009)
[19] TomTom: URL: http://www.tomtom.com (last visited 14. Feb. 2009)
[20] Apple URL: http://www.apple.com (last visited 14. Feb. 2009)
[21] URL: LocateMe 0.4: http://www.soneso.com/blog/index.html (last visited 14. Feb. 2009)
[22] Fire Eagle: URL: http://fireeagle.yahoo.net/ (last visited 14. Feb. 2009)

Information Services

Information services include news, sports, weather, stock, mobile yellow pages and routing assistance. One of the many existing examples of information services is *Wikinear* [23] which, provided with location information, provides users with respective location-dependent location. Further examples can be found in Giaglis et al. [43] p. (67).

Tracking Services

Gruteser et al. [60] mentions experimental automotive telematics applications as an example for location-tracking services. Such applications receive frequent updates of individual's positions and by adding information about the current traffic it is possible to suggest new routes and thus ideally prevent traffic jams. Another service is provided by *WSP live*. It offers a web-based interface to real-time information about the public transport in Helsinki Finland [24]. At this point we refer to one particular part of our implemented platform that is described in chapter 5 (p. 133).

Applications like these are quite useful and beneficial to users. Many location-based applications are conceivable such as asset-, fleet- and logistic monitoring and many more. *GPSGate* [25] is only one out of many examples that allows creation of different kinds of tracking applications, depending on the respective usage scenario. Such applications are already in operation and the society has accustomed to the possibility to track their postal delivery which is a service long ago.

Other commercial tracking services do not refer to locate and track goods but people. With the proliferation of social services and the possibility to include location information, tracking of friends has become an integral part of many social applications. The number of such available mostly freely available applications is unclear. Perhaps the most popular tracking service which went operational during the time of writing this dissertation is googles' *Latitude* [26]. Similar applications such as *Mologogo* [27] of —Loopt [28] which are also free services that can track users with GPS-enabled mobile phones are not as popular as *Latitude* but from a technical point of view quite comparable.

In 2006 google patented 8 patens about tracking [67] [29], a circumstance that points out that huge companies attach importance to tracking related technologies.

Tracking technologies are also investigated in the scientific area. This dissertation shows many different aspects in almost every chapter that localization and tracking seems to be one important aspect for the development of future systems and applications. One such attempt is the undertaken in the project Mobile Millennium. Here cell phones are used as mobile traffic sensors. [30]

[23] wikinear URL: http://www.wikinear.com (last visited: 14. Feb. 2009)
[24] URL: http://transport.wspgroup.fi/hklkartta/defaultEn.aspx (last viewed 5. Jun. 2009)
[25] GPSGate URL: http://gpsgate.com (last viewed 16. Feb. 2009)
[26] http://www.google.com/latitude/ (last visited 14. Feb. 2009)
[27] http://www.mologogo.com/ (last visited 14. Feb. 2009)
[28] http://loopt.com (last visited 14. Feb. 2009)
[29] Die Google-Falle URL: http://www.googlefalle.com/googlefalle/ (last visited 14. Feb. 2009)
[30] project *Mobile Millenium* URL: http://traffic.berkeley.edu (last visited 14. Feb. 2009)

Social Services and Applications

One example that can be assigned to social services and applications and that makes use of tracking technologies with the aim of tracking family members is the *Whereabouts Clock*[35]. The intention of this applications is not to show the precise location of person. Locations are rather categories such as *home*, *work*, *school* or *elsewhere* and allows each member to preserve its privacy if desired. The Whereabouts Clock consists of a display that shows each category as one section of the screen. Each family member has a dedicated icon that is assigned to the respective

The *Whereabouts Clock* is a dedicated rebuilt laptop that shows the categories of interest as a section on the screen. Each family member is represented as icon that is assigned to a category according to her current location. The idea is to emphasis family aspects such as awareness of other's activities which, as the authors describe, contributes to the families' identity.
This is an interesting example in the area of social services and applications. The findings reveal much about certain needs and aspects concerning families with regard to location-based services. In particular, the authors of the *Whereabout Clock* find out that the families' perception on *location awareness* (comp. section 2.2 (p. 13)) differs in that not only the communication of location and activity for supporting the coordination was important. Location-awareness in this sense rather strengthens the emotional connection between the family members by visualizing what each member already knows about the others. So, knowledge about the actual location and coordination amongst family member was secondarily.

Friend Finder Applications

Some of the previously mentioned applications like googles' *Latitude* can be counted to the so called *friend finder applications*. Similar applications like *Dodgeball* [31] that exist meanwhile even for a longer while also allow users to ask for the location of their friends or family members.

But, exchanging location information is not the only information that is shared and exchanged between users. Additional features and communication capabilities are meanwhile standard and allow users to interactively communicate and stay in touch in various ways. Perhaps the most simple solution is to provide a chat so that users can write text messages to one another. Due to missing or reduced keyboards writing messages is sometimes cumbersome. Anyhow, applications such as *Socialight* [32] are optimized for mobile use by letting users leave different kinds of messages, pictures and audio files in specific places by using the existing infrastructure of mobile networks and additional servers that store the media.

The area of location-based applications is huge and it is impossible to list neither all scientific nor commercial applications. Similarly, the distinction between different categories of applications is sometimes difficult or not target-aimed due to overlapping functionalities and braod communication capabilities which render applications being not restricted to one single use case.

[31] Dodgeball URL: http://www.dodgeball.com (last visited 16. Feb. 2009)
[32] Socialight URL: http://socialight.com (last viewed 16. Feb. 2009)

Concluding Remarks on Location-Based Service Examples

The first two examples for emergency services clearly show that the sensor technology is meanwhile on a high-level and already deployed in various kinds of applications. Some applications such as the *avalanche emergency system* exist for meanwhile more than 20 years. In this regard, especially important aspects such as the already existing location localization capabilities with high precision are often overlooked. One of the upcoming challenges is how existing and upcoming technologies can be better utilized. Beside technologies and applications such as the avalanche emergency system, that are rather offside, the most prominent technology which can also be seen as some kind of precursor technology that on the one hand provides many possibilities but on the other hand raises various questions regarding location privacy and data protection is the RFID technology. Of course, RFID can be deployed in many different application areas and the possibility to store and transport and exchange location information with the help of RFID opens many possibilities. But, privacy advocates claim that near field technologies in general also provide a huge potential for misuse. Again, questions like who stores what information when and were have to be answered in alignment with legal regulations and sustainable technology [68].

One important prerequisite for the protection of privacy sensitive data is the design of the overall system. The choice and integration of localization technologies is not subject to newly designed systems only. In fact, the integration of newly available localization technologies into existing solutions should be rethought in consideration of avoiding that one technology intervenes the other and, as a consequence, degrades the overall security and privacy protection of the system.

Another important technical questions that follows is what kind of middleware to use for the realization of location-based services? Or, is it even possible to abstain from middleware at all? It is clear that design decisions like these have also major influence on the trust model. Whereas centralized systems are increasingly suspected to possibly breach security and privacy regulations, systems that do not rely on central servers are rather perceived as trustworthy. Two prominent examples are googles *Latitude* and *peer-to-peer* networks. While the advent of *Latitude* caused worldwide skepticism and fear that google collects location information of individuals, file sharing with peer-to-peer networks that do not rely on central servers were accepted and used intensively. Similarly, *Skype* uses a similar network topology and even proprietary dubious ever-changing encryption of media data which renders its use rather questionable.

2.2.8 Design Patterns for Location-Based Services

In this section we discuss the importance of design patterns with respect to Location-Based Services. Why is this so important and is there a connection to design patterns used in software engineering? Since Location-Based Services are anyhow difficult to capture as a whole the following discussion about design patterns may probably not provide the answer to all questions. Anyhow, the aim is to give guiding principle what should be considered when designing Location-Based Services and analyze different criteria.

Basically, the design of location-based services depends on the respective application. From that, different requirements can be derived that are essential for the operation. Some design decisions are more specific and closer related to the needs of the particular application. Others are rather generic and representative for certain kinds of applications or groups thereof.

Storage and Processing of all Information Users might need on the Mobile Device

We start with one of the most important questions that is where location information shall be captured and processed. In this connection Matt Duckham Matt and Lars Kulik [45] (p. 159) mention an approach which represents rather an extreme, that is, where users carry all the information they might need around with them in their mobile devices. In section 2.4.10 (p. 63) we refer to a system called *Privacy-Observant Location System* which follows this approach with the aim to raise the user's awareness of their location privacy.

Applications that are designed according to this scheme are rather an exception. Duckham et al. [45] cite three reasons why this approach is not viable for most Location-Based Services:

1. The first reason is that typical mobile devices have only limited processing and storage capacities and that this fact renders mobile devices rather unsuitable to be used for computationally intensive tasks. In the course of time mobile devices have developed to multifunctional devices with different communication, high processing power and storage capablities. However, nowadays location-based services may require the processing of voluminous spacial data and rely on the interaction with different services that makes central processing on the mobile or even on one single server rather impossible.

2. The second reason considers the spacial data itself, and in this respect especially the collection of location data. Although GPS is easy to use and well understood, it also has some obstacles. For a detailed discussion about different positioning systems, their advantages and disadvantages we refer to section 2.2.5 (p. 19). As the number of mobile devices with integrated GPS receiver increases, this also raises questions of how this data shall be optimally exchanged between the generator of location data and the system and as a result of this between the users. Different LU strategies are covered in section 5.7.1 (p. 143).

3. The third reason that is mentioned concerns integrity and currency issues when copies of data sets shall be distributed and exchanged over multiple mobile devices.

The example we just discussed refers to the *client-based* solutions and mainly subsume mobile devices that are capable of capturing and processing their location and other privacy sensitive information. Since these applications do not necessarily need to interact with other systems except when the users decides to the protection of sensitive data and hence the users privacy is better than in the case of *network-based* and *networked-assisted* solutions. As an example Schilit et al. [47] refer to applications where users preload their mobile device with different kinds of information that can be accessed and processed later on. However, not only for ease of use but also for the sake of simplicity and finally to be able to provide applications that allow the use of even complex interaction patterns, most location-based services and applications can be counted to either the *network-based* or *networked-assisted* approach, which necessarily also need better means of privacy protection.

Location Update

The next important question regards who requests location information, who receives it and by whom it is processed. In this context Adusei et al. distinguish in [41] between three basic services *pull*, *push* and *tracking*.

- *pull*: Example of customer who sends a request to the particular service number. The customers' identifier is used to determine the location which is needed by some service provider who returns information that related to a specific area.
- *push*: differs form pull in the sense that the service request is not done by the customer but by the service provider. Therefore, the service provider may administer user's profiles which give permission to locate users under specific conditions.
- *tracking*: As in case of pull and push it is assumed that the customer has given consent people or services to not only localize but also track her. If the operator is the service provider at the same time and offers services only to its own customers, the realization of tracking services is relatively easy. However, if this is not the case, that is, if the network operator is not also the service operator the design and operation of location-based services becomes more complex. Furthermore, as discussed in section 4.7 (p. 125), if different network operators shall cooperate and provide location-based services on national and international level, technical, social and legal obstacles have to be considered.

2.2.9 Location-Based Services and Privacy Protection

In section 2.2.2 (p. 14) we discussed the evidence and the expected positive reactions of the markets on the recent developments in the location-based industry. On the one hand, there is certain evidence that the huge potentials in this market segments and the certain omnipresence of location-based services and applications will even in the future have changed our everyday life dramatically. Recent and upcoming technological advances in positioning technologies and advances in privacy protection technologies will contribute to this development. All these efforts aim at overcoming the difficulties and obstacles of protecting the users privacy in the face of rapidly changing technological capabilities to eventually be able to provide also long-term solutions.

Changes of users attitudes are the downside of this efforts. Duckham et al. [69] mention two examples for this. The first one is a bill from 1753 for the establishment of a census in Britain. It was put down as "*totally subversive of the last remains of English liberty.*". The second example points at the vision of a future digital credit system that allows to track every transaction and reason about the users spending habits. These two examples clearly show, that changes of attitudes may even relocate the perception of privacy but does not diminish its necessity.

User studies are an approach that provide important insights how location privacy is perceived. The results of such studies allow to draw conclusions about how users perceive different kinds of applications, interaction models, the sense and attitude to location. As a result, research into location privacy from the users perspective provides interesting results and insights. In the following the most remarkable findings are discussed.

User Studies on Location Privacy Protection

Contrary to popular believe, Barkhuus et al. [56] studies show that people generally perceive location-based services quite positive on condition that they also can benefit from it. In their diary study of rendezvousing Colbert [70] asked students to report the number of friends they would immediately share their location. As a result, many students had ten or more other persons on their positioning list which let the authors assume that these results came from an experimenter effect and decided to not publish their results.

Studies that compare and analyze the perceived intrusiveness between position-aware and location-tracking applications come to the conclusion that location-tracking applications are perceived definitely more intrusive. This result corresponds to the fact, that location-tracking applications and plaforms indispensively require for privacy protection solutions. Section 2.2.6 (p. 24) discusses in detail the differences between position-aware and location-tracking applications with respect to privacy.

We don't agree with their conclusion to put the development emphasis rather on position-aware instead of location-tracking applications. The current success of location-based applications available on the market is indeed characterized mainly by position-aware systems and applications. However, as there are meanwhile many tracking platforms available, developed and operated for research purposes as well as commercial solutions, we beliefe that in the future the technological development will continue to provide improved security and privacy solutions that will significantly enhance the user's trust and confidence also in location-tracking applications. Given that, during the next decade we expect different kinds of position-aware as well as location-tracking applications to become an integral part of our every-day life.

As an example, Burak and Sharon [36] provide a thorough evaluation with a large user group of more than 47.000 users. The survey lasted about 21 mounths and included Instant Messaging and Location, Location-based Chat and Anyonymous Instant Messaging and provides interesting results concering the preferences and likes of users as well as the observed privacy concerns. Their observations revealed that among the provided features most users found location as the most interesting one. However, regarding privacy the results show that the provided privacy tools were hardly used, in total, more than 50% did not use the privacy feature at all. User comments such as *"I don't feel any need to hide myself."*, *"I am not ashamed in my whereabouts"* or *"Hiding? On the contrary - find me, communicate with me; meet me!"*

The observations made by Burak and Sharon are compliant with the results of Barkhuus et al. that were discussed at the beginning of the chapter. However, as Burak and Shaon state, different factors such the young age of the test persons and software specific hurdles that may be decisive for the use of one or the other service also have to be taken into consideration.

In [56] Barkhuus et al. argue that research on privacy primarily focuses on technology. Even though there is a consensus about the importance of privacy, only few research addresses the underlying needs for privacy or the user behaviour. Their research investigates the following questions how users perceive location-based applications (be it position-aware or location-tracking) in exchange for giving up their location information and if location privacy meets concerns. The goal of their study is to find out peoples' expectations and concerns with regard to their location privacy. The studies undertaken by Colbert [70] show that applications with *friend finder features* have the potential to enhance people's everyday tasks.

Junglas and Spitzmüller [40] investigated different services such as *Private ringing profile* where the mobile phone "knows" when the user is in a meeting or in class and a service *Localization of predefined friends* where the mobile phone can locate predefined friends and alert the user when they are within a certain distance. The service *Lunch service* where a suggestion for lunch is pushed by the retailer to the mobile phone when the user is around a restaurant or fast food place was rated as to be least useful and most intrusive whereas the former services were rated as most useful. But, although the localization service was rated useful the results further indicated that it was also perceived as intrusive. Finally, they found that people are generally not concerned regarding their location privacy. The results show that the location-tracking service was perceived more intrusive than the position-aware ones. The results indicate that individuals trade personal attitudes against intrusiveness and perceived privacy. The success of location-based services mainly depends on whether it will be possible to offer systems that cope with partly contradicting personal decisions of individuals and anyhow guarantee privacy [71]. Finally, the term *privacy* is very elastic and section 2.4 (p. 47) discusses some of the most important aspects including the notion of *location privacy*. But, as L. Barkhuus reveals in her studies in [72], users may give their location away as long as the application is cool. This may not connive all the efforts undertaken to build systems that take *location privacy*, which is discussed in the following, for granted.

The Importance of Location Privacy

The widespread use of today's location-based services mainly focuses on position-aware applications such as classic navigation systems. Such systems are available as hardware solutions with embedded software that mainly processes and displays location information received from satellites. By reflecting the classification scheme of location-based systems, it is clear that this kind of application belongs to the position- or location-ware applications. As this kind of location processing basically does not involve any further party, no additional privacy preserving means are necessary. Thus, for this kind of applications location privacy is almost irrelevant.

Next, we consider the case when the same application allows to connect to some kind of remote service. At this point, it is not important what is actually done with the location data or which service is actually provided. The only thing that is important at this point is the fact, that this service is explicitly called by the application and that the current position of the user is transmitted to this service. This case is related to the so called sporadic queries (see section 2.2.6 (p. 24)). Meanwhile most navigation systems provide means that either allow to connect to remote services by means of the mobile phone's GPRS or UMTS connection. This includes both proprietary solutions provided by vendors and third party applications. For example, almost any new car-navigation system enables users to access additional remote services which deliver location dependent information that range from weather information to notifications about upcoming traffic jams or radar control to name only a few.

In this regard Küpper [42] (p. 258) mentions two specific applications which can both be accessed by the same car-navigation system and that show the fine line between where location privacy is an issue and where it is necessarily not. One application allows to protect the user's car from theft. Independent of if this service is provided by the user's trusted network operator or by some third party application provider, neither case requires additional privacy preserving

means since no information is shared with anyone else but the user. The second application provides the user with information about the current traffic condition. The rational behind why location privacy plays indeed an essential role in the traffic application but not in the theft protection application lies in the distinction of what or whom each application actually locates and hence what or who has to be protected. In the case of protecting against car theft not a certain person but only the car is identified and protected. The traffic application however does not only take into consideration a single car. It processes information about many cars at the same time and informs all subscribers that are nearby an event. This requires means that provide location privacy of each individual subscriber.

The abovementioned traffic system represents only one out of many possible examples that refer to location-tracking services (see section 2.2.6 (p. 24)). In comparison to position-aware services or applications, location-tracking applications require much more difficult means of privacy protection. The reason for this lies in the characteristics of location-tracking applications.

The aim of location-tracking systems and applications is to collect and process location information of subjects and objects. This may include lifeless objects and people alike. With the proliferation of pervasive or ubiquitous computing technologies people's movements can be captured with a so far not reached accuracy. So one has to reckon that his movements are stored possibly even for a long time. Furthermore, the tracks stored provide very high accuracy. It can be assumed, that in future stored information is of such high precision that the motion can be rendered close to the actual movement of the past. This may reach down to sub-meter accuracy that is every second [73] (p. 1). There is no question, that such applications may constitute severe privacy risks not only to single persons who use such services but also the whole society that adapts to new technologies gradually. It is also obvious, that all privacy sensitive information that is collected has to be protected. In this regard, location-privacy plays an essential role.

In the previous section we discussed different research results and user studies that aimed at discovering if and to what extend users perceive location-based services as intrusive. To our surprise, almost all research projects that aim to investigate location privacy from a user-centric point of view come to the same conclusion that users are very much concerned about the use of location-based services and, what is more critical, do not seem to care about their location-privacy. In fact, some of the results indicate that the user's attitude towards the use of location-based services and the protection of their sensitive data is in some cases conflicting, even though users are in many cases aware of the possible risks of trading location information by privacy.

As a conclusion on the users mainly airy handling of location information and the observed perception of location privacy that is obviously different from expected we refer to Brown et al. [35] whose long-term field trial of the *Whereabouts Clock* provides interesting insights in family members perception of location privacy which comes to the same results. Based on their results obtained from their clock they ask if privacy is just of researchers concern but does not play an important role for families. Regarding the relatively low privacy concerns of users it is up for discussion if this argumentation is also valid not only for families but for users of location-based services in general?

2.2.10 Conclusions and Future of Location-Based Services

This section concludes the discussion about location-based services and applications and in addition provides a brief future outlook. We discussed in detail various important aspects pertaining location-based services. The discussion started with a comparison between location-based services and context-aware computing, we showed different location technologies and how location-based services can be classified. Examples of location-based services, design patterns and finally privacy aspects concluded this section.

Even though the discussion tries to cover as many different important aspects as possible and we try to show up and answer interesting questions in the field of location-based services, it is clear that for a comprehensive view also other influential developments including non-technical interrogations must be taken into consideration. The following section on business models broadens this view by non-technical aspects and at the same time proposes a new architecture that provides new means of revenue for operators and service providers likewise.

Many location-based services concentrate solely on technical aspects but do not take into account the users social context and their social network. The fact that the mobile phone is a social tool which primary purpose is to connect people with other people is often out of sight [74]. Next generation location-based services must take the next step and avoid being solely based on a pair of geographical coordinates. Users position is indicative of an activity, intention, or goal, but it can be further refined by using the rest of context information about the user, especially their social network: "Are my friends near here?", "Are all these people also attending the event?", "Can anyone around inform me about traffic conditions?". By integrating localisation with context information, location-based services can achieve a higher level of intelligence as it is even perceived by users and evolve to *location-based social services* (LBSS).

Location-based social services enrich traditional location-based services by adding the interaction inside a personal and social context. Whereas location-based services users act rather passively, mostly as consumers and mobile terminals as download-only devices, location-based social services are *user-centric*, that is, the user is contributing to the community and being cared for by the community. No matter what combination of location-based services at hand, if it is reactive or proactive, self or cross referencing, single or multi-target (see section 2.2.6 (p. 24)), location-based social services allow users to be in the role of content creators and providers likewise [37].

This *user-centricity* of location-based social services allows the integration of location information as a kind of user-generated content which can be published and integrated with any other information or content. One such simple example is *blogloc* [75]. This project allows bloggers to show her location to others simply by means of html snippets that are embedded into her website. Equipped with a GPS receiver it is possible to publish location information.

As location-based social services complement with the Web 2.0 paradigm this enables network operators to shift from a closed model towards an open model. Enabling operators to be part of this development paves the way for the implementation of new revenue channels and, on top of that a new starting point for a Web 2.0 business model.

2.3 Mobile Business and Markets

During the last approximately 20 years the mobile phone developed from a high-end business tool to the most widely-used electronic device [76] (p. i). Even though predictions about future developments are difficult, especially the developments during the recent years show, that the mobile business will continue to develop significantly during the next years. In this connection strategic analysis like *Understanding the Mobile Ecosystem* [76] provide a good overview by emphasizing different aspects as to new developments, future predictions and business models which are also discussed in this section.

From the mobile industries point of view this development provides many opportunities for the different involved parties. One important opportunity that the mobile business provides is the possibility to find new ways to generate revenue. The driving force is the possibility to offer services instantly. That means, users are not required to use immobile computers anymore to request services and buy goods. Instead of that, services can be accessed independently of time and location. The internet as the foundation of the e-commerce breakthrough allowed to break up temporal constraints since online stores or auction platforms like ebay do not have closing hours. As a consequence of that the advent of e-commerce further allowed purchases of goods and services with the so called *"second secreen"* (that is the computer), instantly from all over the world. By dissolving the spatiotemporal constrains e-commerce became an important economic factor.

The aforementioned evolution of the mobile phone which is now also referred as the *"third screen"* [76] (p. 5) goes even one step ahead. It is no longer necessary to understand the possibility of determining the actual position of a mobile phone as only an intrinsic part of the network operators infrastructure. Beside location the next generation of mobile phones also allow other contextual information to be gathered such as the intensity of light, acceleration and orientation information. In terms of context-aware computing, the actual location of a user represents probably the most important and representative variable. It is already foreseeable that in the near future contextual information and the processing thereof gains significant importance for the realization of future mobile applications.

However, since well known business practices such as currently applied in the desktop internet world are not directly applicable to the mobile world, entrance into this market is sometimes difficult. This is also reflected by the unclear and unstable mobile value chain which brings even other players that are ever since located outside the telecommunications industry to the scene. Of course, generally this is not a disadvantage. In many cases this development stimulates market forces and hence provides new opportunities and sources of revenue. But also network operators strike new paths. They no longer exclusively concentrate on provisioning their network infrastructure but also start to serve as content providers. In the next section we discusses why such conglomerations stir up discrepancies between network operators and service providers and the negative effects that raise especially in the location-based service market in Europe.

The so called "closed wall" strategy that most network operators follow in Europe definitely inhibits the development of a variety of context- and location-based services. The value chain in Europe is not as clear as in Japan. Quite different from the practices in europe,

japanese network provider like e.g. NTT DoCoMo[33] encourage service providers to develop services and provide content. Strategic alliances such as between NTT DoCoMo and Google [77] aim to provide new search functions to mobile users. This change from NTT DoCoMos business policy as full-range supplier which includes both infrastructure as well as services was nevertheless necessary to accomplish the raising customers demands. This leads to an increased use and workload of the network and commissions for the service providers [78] (p. 209).

After this introductory words this section continues with a brief overview of the current situation of the mobile location-based market. We also focus on one particular characteristic that is the location-based market.

2.3.1 Location-Based Market

Against all conflicting opinions and business analysis during the last years, the mobile location service market still prospers and it is expected that this branch of industry will grow further to eventually become a billion dollar market already in the next decade. Only recently, in April 2008 the council of ministers of the EU-Parliament authorized the financing of 3.405 billion euro for the first European navigation system Galileo and EGNOS (European Geostationary Navigation Overlay Service) [79]. This represents only one signal example out of many such similar ongoing huge prestigious projects. Examples of recent projects are the Chinese *Compas*, the Indian *IRNSS* (Indian Regional Navigation Satellite System) and the Russion *Glonas* (Globalnaya Navigatsionnaya Sputnikovaya Sistema) which is already in operation.

It is obvious that such huge efforts reflect the need for reliable satellite systems that provide a high level of accuracy and precision of location information which in turn fosters the development of new applications.

Beside such high-tech enabling technologies the mobile business field in general combines a number of different players and complex relations between them. A variety of applications can be operated on top of such high-tech systems and covers the whole spectrum from military applications to civil air space and transportation services to name only a few. Aside from professional applications also a stimulation of the desiderated push to the civil location-based market is expected. The success of each such project is thus of significant importance.

From the mobile data perspective it is the infotainment area that is likely benefit most from the rapid developments of mobile data growth. Market predictions allow the assumption that infotainment will gain significant share by 2011. One way to exploit the unique capabilities of mobile devices and boos mobile data exchange is to allow infotainment to incorporate location-based information. [76] (p. 7, 8). However, market predictions and the quite promising development of navigation systems cannot belie in the fact that, from a present-day perspective, the location-based market is either still in its infancy or just struggling. The success of location based services and applications surely depends on various

[33]NTT DoCoMo is the world's leading mobile communications company. DoCoMo serves over 53 million customers, including 42 million people subscribing to FOMA, launched as the world's first 3G mobile service based on W-CDMA in 2001. DoCoMo also offers a wide variety of leading-edge mobile multimedia services, including i-mode, the world's most popular mobile e-mail/Internet service, used by more than 47 million people. With the addition of credit-card and other e-wallet functions, DoCoMo mobile phones have become highly versatile tools for daily life. from http://www.nttdocomo.com/pr/2008/001385.html (last viewed 7. Jul. 2009)

factors such as the relationship of different stakeholders and the matching of innovation and real market demands [43] (p. 80). One of the most important questions is how different players can generate revenue and benefit? The recent developments during the last years have led to an unexampled proliferation of mobile devices and hence the development of mobile applications that allow users to communicate, exchange and share almost any kind of information such as voice, speech and data. All this is possible while wandering around. Some of these mobile devices are meanwhile capable of dead reckoning their position by means of e.g. WIFI (see Section 2.2.5 (page 19)). But, the coverage of mobile networks and the inherent possibility to determine the location of mobile users seem to make mobile network operators predestined provider of location-based services. But over the years mobile network operators learned that the users demands are obviously different. When network operators started to offer location based services one of the most important lesson learned was that customers do not use location-based services with the expected regularity. At this time the enablement of businesses that allow operators to offer timely personalized and location-specific services finally turned out to be be not as successful than expected [80]. One simple reason lies in the fact that the regular use of applications is a decisive decision criterion for operators whether services operate cost-effective or not or if they generate enough revenue.

The following section provides an overview of the different actors that are involved in the mobile business and their relationships. In particular, by examining each parties interests we also try to identify the critical factors that are crucial for a market introduction. Also interesting research perspectives as well as open issues are pointed out. In this regard, we propose a new service architecture that fulfills many of the deficiencies that can be identified of todays existing models.

2.3.2 Different Actors in the Mobile Business

According to a general accepted classification of three main classes *technology application* and *network* this section provides an overview of the key actors that are decisive in the mobile business market. As stated by Camponovo and Pigneur [81] this classification is not intended to give a complete view of the mobile landscape and should therefore be complemented by *regulation*, *end-user* and *enabling services*.

Camponovo and Pigneur [81] provide their classification framework which has at its center the users needs and the building blocks *technology* (device manufacturers and equipment vendors), *services* (content and application providers), *communication* (mobile network operators and internet service providers), *regulatio* (regulation authorities) and *users* (consumer groups). In the following we briefly discuss the business models of each actor.

Device Manufacturers are so called technology players and produce the hard- and software for mobile devices. As Camponovo and Pigneur [81] distinguish between primary and secondary actors, device manufacturers can be subsumed to the primary actors. Secondary actors are device retailers, component makers, software platform vendors that provide operating systems, browsers and development platforms. In the mobile industry the device's manufacturers value proposition is to provide mobile phones, PDAs or notebooks to the end users who should then be able to access mobile networks and run mobile applications.

Equipment Vendors They provide the physical and logical core mobile network infrastructure as well as infrastructure related services. Their competences include everything from designing and building up the hardware and network infrastructure to all operational tasks. Their customers include mobile network operators as well as Internet Service Providers.

Mobile Network Operators and Internet Service Providers purchase from infrastructure vendors to provide ubiquitous communication services and access to their and other networks. Especially mobile network operators may further provide also network-related information such as the location information and identification of users and billing services to third parties. In order to allow customers also access networks of other network operators and the internet, they have to set traffic arrangements with other network operators and service providers. Another important matter for mobile network operators is the distribution of handsets which is one means of advertising and the foundation for a valuable customer base. The revenues of mobile network operators are a combination of traffic arrangements and granted subsidies to customers as well as a combination of subscription, airtime and volume-based fees. Similar to mobile network operators, internet service provider partner with a range of different actors. This is essential for the development of the 3G market and for increasing revenue.

Content Provider generally process and further distribute data via different channels to customers. This includes multimedia data such as music, videos but also news, location or presence information to name only a few. Depending on the respective application at hand content provider collect, aggregate, format, publish or distribute any related information so that it can be further processed by content aggregators, portals or network operators and finally consumed by users with their mobile devices.

Application Provider take a diverse role. They mainly provide applications that are hosted on dedicated platforms. Such applications may be composed of a number different applications that are distributed and accessed remotely. There is sometimes a tight relationship between application providers and network operators. Especially when application providers obtain sensitive information such as location information.

Payment Providers provide a variety of payment methods allow cash-free purchases of goods and services to customers. In the mobile business different payment agencies are conceivable such as credit card companies or smartcard companies to name only a few. Other payment agencies have specialized in the accomplishment of online (mobile) payment. Especially mobile services are usually charged directly via the network operator. All these payment methods have in common that have partnerships with one or more financial institutions which perform the actual financial transactions.

Users are to some extend the most critical part. Their decision directly influences the skills of all the players and determines whether the mobile business is a success or not. Two different kinds of users can be distinguished. One kind relates to business, whereas the other one addresses the end consumers of mobile services.

Regulation Authorities are an important market instrument that constrains all players by setting up legal and social frameworks. Anyhow, these authorities have no direct influence in the provision of services but their decisions may result in major effects in the market.

2.3.3 Business Models

As already mentioned in the introduction of this chapter, business practices of the desktop internet world cannot be directly applied to the mobile world. As Camponovo and Pigneur [81] state, *mobile commerce* is often confused with *mobile business* which is understandably unconducive for the development of mobile location-based services and the mobile business as a whole. For that reason we first give a concise description of what a business model is. Therefore we glance at some business model definitions to provide a better understanding of the matter.

What is a Business Model?

Camponovo and Pigneur [81] cite different definitions of business models. The first one describes a business model as *"the logic of a business system for creating value that lies behind the actual processes."* (Petrovic et al. [82] cited in G. Camponovo and Y. Pigneur [81]) which can be seen as *"as a detailed conceptualization of an enterprise's strategy at an abstract level, which serves as a base for the implementation of business processes."* (G. Camponovo and Y. Pigneur [81]).

Apart from this general view they also cite another definition that considers rather the elements a business model is composed of. This definition describes a business model as *"the totality of how a company selects its customers, defines the tasks it will perform itself and those it will outsource, configures its resources, goes to market, creates utility for customers and captures profit"* (A. J. Slywotzky [83] cited in Camponovo and Pigneur [81]).

The following definition: *"A business model provides a description of the roles and relationships of a company, its customer, partners and suppliers, as well as the flows of goods, information and money between these parties and the main benefits for those involved, in particular, but not exclusively the customer"* (Bouwman, 2002 cited in Camponovo and Pigneur [81]) is quite similar to the previous one.

One way to understand what a business model is and what it should consist of is to compare them. In order to better understand the currently deployed Telco's business models with other business models in the same industry, Osterwalder et al. [65] systematically compare traditional Telco's business models with so called disruptive technologies such as Skype. During the initial phase of the live cycle of disruptive technologies the performance and functionality is usually not as high as compared with established technologies. At this stage these technologies usually provide services for free or at least at lower prices. Improvements and innovative features contribute to further distribution which implicates an introduction on the mainstream market which, in an extreme case, may lead to an displacement of the incumbent by the disruptive technology.

In order to be able to describe, compare and analyze two business models in a structured and systematic way, Osterwalder et al. [65] apply business onthologies. The use of onthologies

allow to explain *what a business model actually is and of what it consists*. Referring to the definitions of business models and its elements, onthologies are means to provide definitions of those companies elements that are critical for the operative result of the company. Examples for onthologies that can be used for the formulation and description of the companies' elements and relationships are e.g. the Business Model Onthology (BMO) (Osterwalder 2004 cited in [65]) or the v3value onthology (Akkermanns, Baida et al. 2004 cited in [65]). The BMO uses nine elements such as the business model's *value proposition*, *recources and capabilities*, *partnerships*, *cost structure* and the *revenue streams*.

The focus of the following discussion about possible business scenarios is restricted to the main players in the mobile business that are the network operators, the application providers and the users. This view on business scenarios in location-based services is in line with the discussion about this issue by Ramaprasad and Harmon [80].

Network Operator-Dependent Business Scenario

As starting point the network operator represents the exclusive source of location information for location-based services. This scenario requires operators to be in charge of the appropriate platforms, applications and interfaces that are necessary to provide such services. In this scenario, the network operators provides only the location information of users that is anyhow available as this is a network intrinsic information. Given the appropriate interfaces provided to access location information of the network operators users, these service providers instantly benefit from a huge customer base. Customers who are looking for location based services that use the localization capabilities of the network operator are forced to access only those applications that are under the exclusive control of or at least controlled by the network operator. As a consequence, this scenario suppresses market forces and hence both a viable range of applications to chose from and market-driven prices.

An important question is how operators can gain additional revenue. Location-based services that are operated in a network operator-dependent business scenario generate similar revenue streams like voice-services. Depending on the location-based service at hand, different pricing schemes are conceivable. Examples range from a monthly fee, pay per usage, air-time-usage and packet-usage. In case location-based services are offered by third party service providers, the network operators may gain from transaction or fixed fees.

Network Operator-Assisted Business Scenario

The second business scenario is similar to the one described above except for that this time it is further assumed that the network operator relinquishes exclusive control over location information. This allows more location-based service providers to enter the market which in turn stimulates competition and forces applications that are not successful to withdraw. However, the downside of this developmnt are confusing pricing schemes which result from inconsistent billing infrastructures. Customers have to face the whole bandwidth between price excesses and aggressive dumping. It may be difficult for customers to judge the real value of applications.

Critical factors such as security and privacy protection, the ability to adapt who may access the own location information according to ones preferences address only the very basic requirements most users expect from applications. Provided that the these critical factors can be fulfilled, application providers can assume that users trust their applications which is essential for the success of location-based services and applications.

Network Operator-Independent Business Scenario

The last scenario refers to mobile devices that are independent of the network operator in terms of location information retrieval and processing of location information. As with the advent of mobile devices that have integrated GPS receiver and the myriads of existing navigation systems that use GPS (also including mobile phones) it seems that operator-independent solutions may even outplay network operators as competitors on the location-based services market. Some products that allow to track goods, vehicles or children even rent capacity of network operators. In these cases, customers are not necessarily aware of the underlying network providers. This development raises the frequently asked question if network operators may in future become low-cost data pipes[34]. But, for network operators, also 3G bandwidth-hungry services can be a problem. Tiller [84] cites that in 2007 Telenor reported that bandwidth of a single cell was just enough to serve the data-transfer rates of two users watching a live video stream of a football match.

Other bandwidth-hungry services such as watching YouTube[35] videos on mobile devices clearly show that higher bandwidth is a critical success factor. Tiller further cites that HSDPA (High Speed Downlink Packet Access) seems to fulfill these requirements. Time will tell if a 10-fold increase in data traffic can be achieved by mobile networks in 2012.

Most future mobile phones that are capable of HSDPA also allow using WLAN, Bluetooth or other near-field technologies. Also GPS receiver and compass that allow a number of things such as precise localization, orientation and different media access possibilities. A number of emerging free Wifi networks[36] alleviates the development and propagation of network operator-independent solutions.

2.3.4 Definitions and Interpretations

Although the widespread use of location-based services, there are still only a few successful deployments that represent an exemplary function with respect to revenue gain and increasing profit. One possible reason why there are also only a few known studies with the explicit concern about location-based services may perhaps lie in the fact that, as J. Raper *et al.* [20] (p. 29) states, location-based services are services like any other services available and thus subject to the same range of business models with similar success factors. One requirement that determines one such success factor is the need to provide services that are compelling enough to be used recurrently. However, operators argue that the end-user behavior does not pay off the investments that are necessary for the operation of location-based services.

[34]Mobile operators analysis: http://www.analysysmason.com/About-Us/News/Newsletter/Previous-news-articles/Are-mobile-operators-rapidly-becoming-low-cost-data-pipes/ (last viewed 19. Feb. 2009)

[35]URL: YouTube http://www.youtube.com/ (last viewed 19. Feb. 2009)

[36]list of free networks: http://www.freenetworks.org/ (last viewed 19. Feb. 2009)

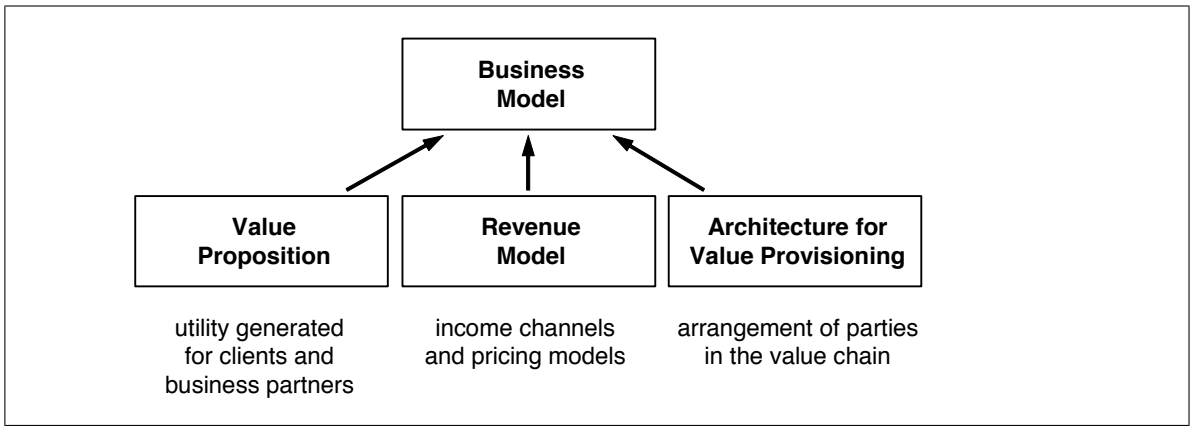

Figure 2.2: Business Model

Services such as those that allow to inform about nearby gas stations, tobacconist's or cash machines are either only used on an irregularly basis or never. To generate enough revenue, such services must be used several times per week. However, since people most of the time know the surrounding environment very well, such services are not needed. During holiday or while traveling, many users may simply forget to use such services. And even when users subscribed to navigation services high roaming costs may impede further use of services outside the operators geographical domain.

In this context Giaglis et al. [43] (p. 79) mention the so called *pararadox of mobile location services* which refers to location-based services that are used rather in a local environment. However, for many location-based systems service portability and roaming issues are still not solved properly to provide location-independend and transparent services to users.

The service architecture proposed in this dissertation is one necessary building block for the constitution of a *business model* as it is discussed by Figge and Rannenberg in [2]. In addition to the architectural design, this model further comprieses a *value proposition* which refers to the utility that is generated for both, clients and business partners likewise, and a *revenue model* which defines the income and pricing models. This business model is also shown in figure 2.2. Although Figge and Rannenberg focus on a new revenue model for multimedia services, this business model can be applied to the location-based service architecture proposed in this dissertation. The following discussion refers to Figge and Rannenberg and illustrates the the value proposition of current mobile commerce applications.

Current Business Model in the Mobile Telecommunication Market

The typical mobile commerce business model is characterized by mobile portals provided and operated by network operators. Examples of such portals are i-mode, Vodafone life! or t-zones to name only a few. The revenue model of i-mode model is applied at most of all. It allows mobile network operators to receive commissions on revenues that are generated by the portals. Whereas the i-mode model in Japan provides various services for customers and generates high revenues, the European market is primarily dominated by mobile voice, messaging and data services. Despite the hope that the establishment of portals increases

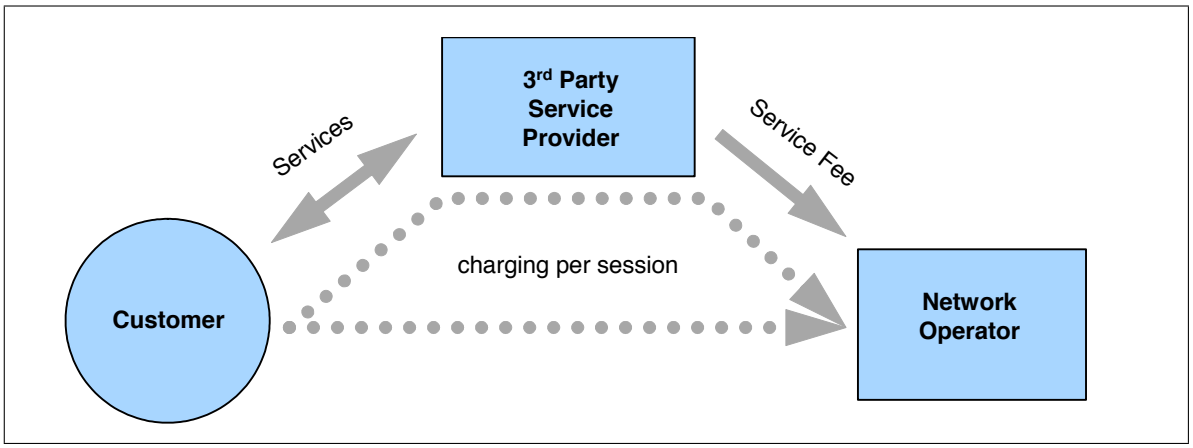

Figure 2.3: Hitherto Business Model [2]

revenues, most services offered are not adopted by the customers. The main reason for that is that customers are charged for mobile data traffic and hence for every single service request. Thus, to spare traffic and in turn costs, customers tend to select and use only those services that bring immediate value.

Figure 2.3 shows the current business model that is nowadays applied in the mobile commerce scenario. The deficiencies of this model are best explained by the crucial factors that decide over success or failure of the adoption of mobile services that are *usefulness*, *usability* and, as already mentioned above and referred as the most decisive factor why services are consumed in a minor degree, the *costs* being spent by customers. The following explanations refer to the business model as it is depicted in figure 2.3. First, it is assumed that mobile network operators provide portals that allow users access to mobile services. The desired benefits of such portals were already discussed above. However, the disadvantages of the implemented revenue models of such portals are mainly driven by the fact that mobile data is charged per session and that almost all services are provided by the mobile operators themselfs. This leads to the fact that customers select only those services that provide immediate value. The most obvious conclusion that can be drawn is that services that primarily provide value for 3^{rd} party service providers that are outside the domain of the network operator are not feasible.

Meanwhile a trend that introduces a new business model becomes apparent. This trend may have the potential to extend or even replace the traditional business model which current network operators are stuck with. The result of this trend reversal first results in more flexibility and competition and and second in higher expected revenues. We will discuss the details about the proposed business model in the next section.

Proposed Business Model

One of the first visible steps towards a new business model that overcomes the deficiencies that mobile network operators have to face currently is the introduction of standardized interfaces such as Parlay X 2.0 [85]. In general, these interfaces allow application developers to make use of network operators service enablers such as group lists, presence, instant messaging and location to name only a few. The introduction of Parlay X shows not only how such

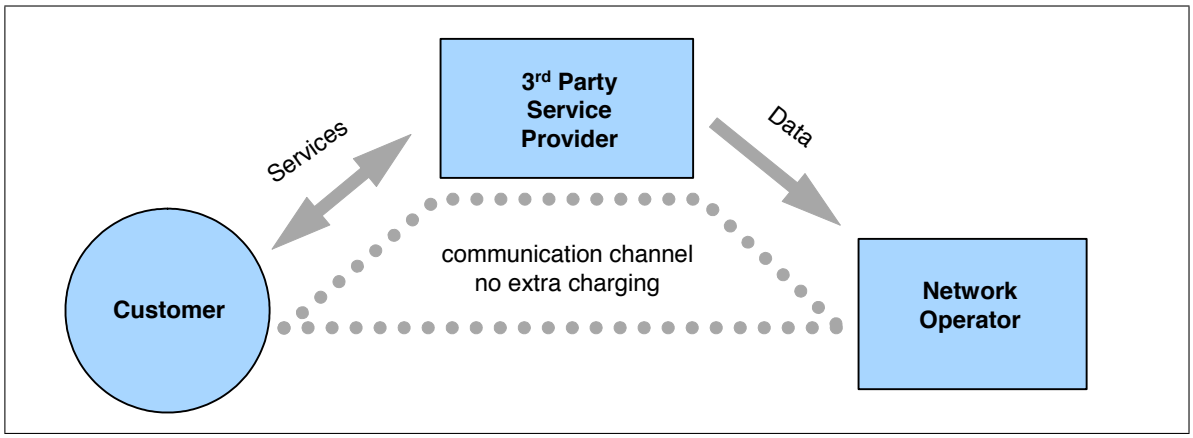

Figure 2.4: New Business Model [2]

interfaces allow 3^{rd} party service providers to make use of the manifold services that were so far only available to the operators. This introduction allows the integration of anciently excluded 3^{rd} party application providers and in addition provides significant benefits to all involved parties. As a result, if network operators start to open their interfaces and allow 3^{rd} party service providers to access formerly hidden service enablers, new business models emerge that provide indirect revenue, leverage mobile service usage and thus stimulate the mobile market. Figure 2.4 sketches the new business model where users are not charged for transferred mobile traffic data. This allows to first investigate if mobile services are useful or not instead of drawing rash conclusions based on imperfect information about these services. Thus, the positive effect of this business model is on the one hand that the more services providers emerge on the mobile application market the more competition takes place which in turn results in better quality of services. On the other hand, users have more time to investigate the offered service, evaluate the pros and cons and then decide on the basis full information. This further makes possible advertising and promotion of new services as well as the implementation of customer loyalty programs for mobile applications to name only a few. In a later section the proposed business model is revised. We will in depth discuss the technical realization and discuss another important factor that is crucial for the success of the business model, that is trust.

2.4 Privacy

There is certainly no single answer to the question "*What is privacy?*" and even though the simplicity of this question, the answer is so much harder to find. One of the most influential definitions of privacy developed by the no less famous privacy pioneer Alan Westin [86] states:

> "*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others.*"

This definition as well as the famous quote of Louis Brandeis as introduction of this chapter are without any doubt still valid in todays society. However, various different viewpoints, cultural, historical and legal aspects as well as ethic questions have to be considered to form an understanding of what privacy is. And as the quote further suggests, the *right to be left alone* reflects the *right to privacy* and this inherently depends on the situation and the affected parties. That's why privacy was certainly not invented or even caused by computer or any other modern technology only[87] (p. 603). But, with the advent of the internet and hence the possibility to store and search in tremendous data pools that are accumulated with rigorous data collection, suddenly almost every citizen of the so called information society is affected. The collection of data and the processing thereof is certainly not a new phenomenon. Ever since computer were used to support administrative processes, data was collected and stored. In the former days, when it was not possible to exchange data as it can be done today, technical solutions conforming to legal specifications were sufficient enough to provide and protect the citizens privacy demands. Today, technology relieves us from many burden and allows us to communicate in various ways. However, the vast developments during the last twenty years with regard to technology and the price decline for computers and communication technologies also introduced a number of possible privacy threads without careful anticipation of the social conscience.

Today a vast number of communication technologies exist. With the advent of the so called Web 2.0 phenomenon hitherto internet communication technologies including chat, VoIP, Skype were enhanced by blogs, a kind of digital diary, social network platforms, virtual places and worlds where individuals and companies can find people with the same interests, meet other people or even earn money. The so called Web 2.0 phenomenon, an architecture of participation, comprises various such new social platforms and technologies and in addition allows anyone to create individual combinations of services which result in new ones. Services that are composed in this way are also referred to as *mash-up*s. Individuals are not only encouraged to create new services but also to provide the content. Since *user-centricity* is an important concept of the Web 2.0 it comes easy to users to provide personal data. By feeding the web with personal data, it allows people to not only communicate with each other but to exchange information about themselves which in many cases results in some kind of self-expression and even publishing of very intimate information. Obviously, there is no doubt that many users, especially the younger ones, underestimate or even ignore the fact that their data will be accessible for many years. Photos, videos and texts may be hindering even many years later when looking for a new job or one makes an application for a certain position.

Many people are apparently not good enough informed about the possible consequences that may occur when private data is unveiled to e.g. social platforms like *myspace*[37] while others even simply neglect possible consequences. Personal meanings published to public sites are stored over years and it is difficult or even impossible to delete such entries. Once information is publicly accessible it can be copied and published or conveyed to other platforms without knowledge or acceptance of the author. Meanwhile there are known cases of people who were refused for jobs because of relevant personal profiles offered by them on social platforms. It is obvious that operators of such platforms are busy in conveying the impression that the users privacy is protected. However, as an example just recently discussed in the

[37] myspace: http://www.myspace.com (last viewed 6. Mar. 2009)

Figure 2.5: Vision of Google 2084 [3] (p. 12)

public, a new feature *Beacon* provided by the social platform *facebook*[38] shows clearly how the users privacy is invaded by sending out notifications to the users friends about online purchases from partner websites. The following vehement objections against this doubtful feature forced facebook to react. It is still a questionable matter why users are explicitly required to opt-out instead of providing rather the choice to opt-in to this service. The conclusion of this is that no matter if the user opted-out or not the platform still collects all available purchase information about users with the only difference that once opted-out friends are now not informed about purchases anymore.

Another example for data collection in huge quantities is google. More than 50%, about two thirds, of the search in the US is done with Google. The same applies to Austria. As one may say, Google *is* the web, or, it indicates that Google may in future take a controlling position. The issue gains even more brisance as Google meanwhile also offers various kinds of applications, including text processors, spread sheet, calender, photo album and mail. Contrary to the anonymous search logs, this data is associated with a unique identifier, the Gmail address. Eventually, with *Gmail Paper*[39] Google delivers printouts of Gmails to the postal address of Gmail users and can thus link the Gmail identifier to the name and address of a particular individual.

Many people overlook that also the rights of all documents including texts, photos, videos, emails that are stored on Googles servers are automatically passed over to Google. Except for shopping lists which are not to be sneezed at since Google learns about shopping habits, in case of patents the issue may have serious consequences for the author.

[38] facebook: http://www.facebook.com/ (last viewed 6. Jul. 2009)
[39] Gmail Paper: http://mail.google.com/mail/help/paper/ (last viewed 6. Jun. 2009)

Other initiatives such as the Google Phone[40] that uses the Android platform[41] push on the mobil sector. NTT DoCoMo plans to use Android as its new operating system by 2010 [42]. The example shows, that the competition for supremacy on the mobile sector has already begun. The inclusion of location information provided by users is another little step towards new Location-Based Services offered by Google. However, aggregation of vast amounts of data and the development, refinement and application of data mining technology have raised controversy discussions and alarms by privacy advocates. Googles Library project as well as the aim to collect genetic information for a gene catalogue and a genetic database are perhaps the most prominent examples that prick up ones ears.

A very comprehensive overview about the various issues related with Google provides Maurer et al. [3]. Figure 2.5 was obtained from this document. It gives an idea, at least from present-day perspective, what could be of interest to users and what research has to be conducted for the realization of such services. Of course, this picture is rather a joke, but the message behind is clear.

Apart from the above examples of worldwide accessible applications that allow people to publish their private data also regulatory frameworks are subject to changes, unfortunately such changes are not always in favor of the users privacy protection. One example represents the data retention guideline which obliges internet providers and mobile network operators to collect and store data of their customers.

2.4.1 A Short Historic

As mentioned in the introduction of this chapter, privacy was recognized even long ago as an important social asset. The juridical system of England and Wales for example can be traced back to the year 1195. At this time the *Kings Peace* was controlled by knights that where commissioned by Richard I to preserve peace in unruly areas [88]. The *Justices Of The Peace Act* (1361) which was of importance for the judicial work during the following 600 years bound over unruly persons and served for people offending each other to rather *be of good behaviour*. The act operated on the local level of the country. Its purpose was amongst many others to fix wages, build and control roads and bridges and generally services that were necessary for the welfare of the country [89]. In the light of of privacy probably the most cited passage refers to sentences for the arrest of peeping toms and eavesdroppers [88].

Another well known quote is that of Wiliam Pitt the Elder (1708-87) who was the 1^{st} Earl of Chatham:

> "*The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail - its roof may shake - the wind may blow through it - the storm may enter - the rain may enter - but the King of England cannot enter! - all his forces dare not cross the threshold of the ruined tenement.*" [90]

which expresses in a sensitive way that every man's home is his castle.

[40] Google Phone: http://www.google-phone.com/ (last viewed 6. Jun. 2009)

[41] Android: http://androidcommunity.com/ (last viewed 6. Jun. 2009)

[42] NTT DoCoMo to strip down mobile OS; Android coming in 2010: http://www.google-phone.com/ntt-docomo-to-strip-down-mobile-os-android-coming-in-2010-24298.php (last viewed 19. Feb. 2009)

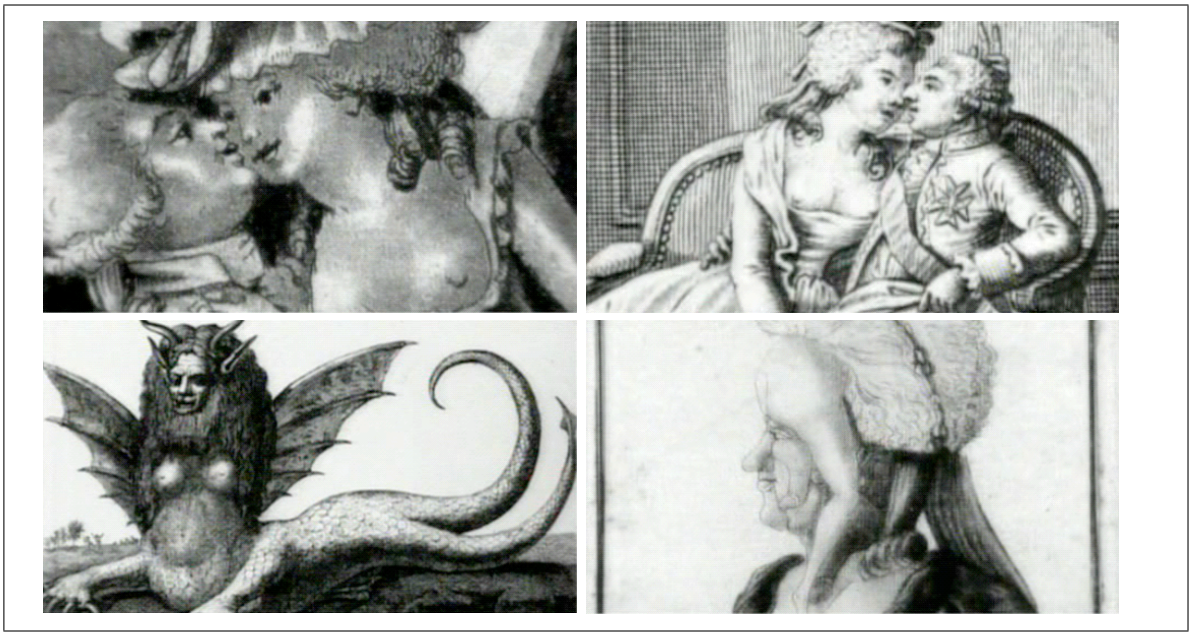

Figure 2.6: Pamphlets against French Royal Couple Marie Antoinette and Ludwig XVI [4]

A meanwhile historical example that aims to find an answer to the question of how the world can look in the future without privacy was given by Louis Brandeis and Samuel Warren in their essay *"The Right to Privacy"* [91]. The motivation of writing this essay was the advent of new cameras that for the first time allowed to shoot photos without the necessity to sit still in front of the camera for a certain period of to time. Brandeis and Warren foresaw this new technology as a severe thread and argued that by enabling everyone to shoot photos of other persons which can then be published in newspapers, social privacy is happen to be violated and this may provoke dramatic consequences.

One such dramatic example that reveals the power of pictures has happened even long before the essay was written. There is talk of the last french royal couple Marie Antoinette (1755-1793) and Ludwig XVI (1754-1793). The famous necklace affair that happened in 1785, was the foreplay of the revolution and a turning point in her life, showing her the reality beyond life in the castle. At the times when the revolution was already in progress and thus the royal cesura was rendered almost inoperative, new hostile pamphlets that were even more aggressive than those that were already in circulation for some years eventually diminished the anyhow wounded prestige of the royal family and especially that of Marie Antoinette. At these days she was called *Madame Deficit* and even worse she became blamed for almost any grievance. Paradoxically, the hate against her culminated with the introduction of the freedom of press, ending of serfdom and proclamation of human rights[43]. Finally, these pamphlets were even responsible for a burst of hostility towards women by demonizing them as insatiable monster. The royal couple did not understand the power these pictures and at the end all undertakings to fight them to keep their royal dignity failed.

[43]Declaration of the Rights of Man and of the Citizen: http://www.hrcr.org/docs/frenchdec.html (last viewed 7. Jul. 2009)

These historical examples show, that the protection of individuals' privacy is not an invention that is associated with the advent of modern information technology. Privacy is rather a basic need that has to be protected.

One of the most important prerequisites needed is an adequate legal system. The first data protection law in the world was initiated in Germany Hessen, Federal Republic of Germany, 1970 [92]. This law was the initial initiative for a number of following data protection laws in different european countries continuing with Sweden in 1974 [93]. In the following section we continue this discussion about privacy legislation in europe.

2.4.2 Privacy Legislation in Europe

The European Union Data Protection Guideline discusses confidentiality and security as well as the processing of data (be it automated or not) in the European Union Data Protection Guideline Directive 95/46/EC (1995) [94]. *Article 13* states several exemptions that under certain conditions the member states are allowed to adopt their legislative measures if it is necessary to safeguard national and public security, defense, various aspects related to criminal offenses, financial and economic interests of the member states or the EU to name the most important ones. From a privacy point of view in the light of these exemptions the critical part still represents the used technology [68]. *Article 16* discusses the issue of confidentiality of processing of personal data from a technical and organisational point of view whereas *Article 17* deals with security and processing of professional data and the legal constraints. Negotiations between European member states about the processing of data and privacy led to a directive Directive 2002/58/EC (2002) [13] (EU Directive on Privacy) which was issued in 2002 an represents an extension. It provides a wider scope on privacy and electronic communications and establishes *technology-neutral* legal standards

Different to the confusing legal situation in the US which was caused by missing regulatory guidance, the European Directive covers the protection of personal data not only for mobile phones but for all electronic communications. It requires that subscribers who want to use telecommunication services that make use of location information give their informed opt-in consent. In addition to the required consent of the user, *Article 9* states that, location data *" ...may only be processed when it is made anonymous and to the extent and for the duration necessary for the provision of a value added service"*. Furthermore, subscriber *" ...must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication or to withdraw their consent for the processing of traffic data at any time.* Another important point is that *"the service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service"*. As denoted in the following, the EU Directive on Privacy distinguishes between *Traffic Data* and *Location Data*. We discuss these two kinds of data in closer detail in section 2.4.5 (p. 58).

Traffic Data means explicitly describes data as *"...any data processed for the purpose of the conveyance of a communication channel on an electronic communications network or for the billing thereof"*.

Location Data is *"any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user or a publicly available electronic communication service"*. It may also refer to the latitude, longitude and altitude of the users terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded. Location data other than traffic data is regulated to the same extent as traffic data.

Price states in [95] that software systems must be jurisdiction aware. This is indeed important but not easy to achieve since privacy regulations vary. One requirement is that the system provides users information about other 3^{rd} party providers who receive this data and for what purpose, data usage and the time span the location data is used. As a result, the owner of data must have sole control. The situation becomes even more complex if data is processed in different countries. Therefore, the European Directive on Privacy and Electronic Communications defines the *transitive closure*. This prohibits data export to countries which do not provide equal data protection guidelines or provision of special contracts. In [96] Fischer-Hübner states that from an international point of view and in the context of a global information society the EU Directives do not provide sufficient privacy protection. Fortunately, the number of countries outside the EU that start to adopt their laws to be conform with the EU Directives is growing [9].

EU Directive on Data Retention

The European Directive on Privacy and Electronic Communications [13] has been amended in February 2006 to protect against terrorism and organized crime. The result of this was the EU Directive on Data Retention which is also known as European Directive 2006/24/EC (2006) [97]. The underlying idea is to achieve an EU wide harmonization of provisions that aims to protect against terrorism. To achieve this, each EU member state is obliged to define appropriate rules and regulations and apply them to their respective national legislation such that access to *traffic data* (see Section 2.4.5 p. 58) is guaranteed. Another change that comes along with this Directive is the amount of traffic data that has to be stored. This has considerably increased just as the retention period. The respective retention period depends on the the data and varies between the minimum retention period of six months to the maximum which is two years.

This regulation affects all service providers of the telecommunication industry, including mobile and fixed-line but also internet service providers, cable and satellite providers. Data that has to be retained includes: phone calls (successful patched through and attempted calls), the time, date and duration of the communication as well as the *location information* (see section 2.4.5 (p. 58)) that is necessary to provide the service.

The Data Retention Guideline has raised many controversies and it remains to be seen if the huge investments really prevent from terrorism as it is assumed [98]. Global players

such as Google, Skype and Yahoo also provide kifferent kinds of communication services on the internet. Some software service provider like *fring*[44] combine different technologies and protocols in one client. Services like Skype use proprietary interfaces and attempts to understand how Skype works, not to mention how communication could be eavesdropped, failed so far. Not only that such services are freely available but also prevents from legally authorized access to communications which is also termed *Lawful Interception* [99]. In the face of such internationally services that, due to the lack of international legislation are definitely not ascertainable by EU regulations and cannot be impeded, it is arguable whether measures like the Data Retention Guideline have any effect [100].

2.4.3 Protocols and Standards

In the following, we present short descriptions of some important protocols and standards which are listed by Mohapatra and Suma [101]. They further mention the International Earth Rotation Service (IERS) which investigates the earth rotation and reference systems such as GPS and other observation techniques[45], *Global Spatial Data Infrastructure* (GSDI)[46], G-XML[47], ISO/TC 211 *Geographic information/Geomatics*[48] for standardization of digital geographic information, *Earth Observing System Data Information System* (EOSDIS) which provides information that is captured by a number of satellites to the *Earth Science Data and Information Project* (ESDIS)[49] controlled by NASA, the *Open Location Service Initiative* by Open Geospatial Consortium Inc.[50], GeoVRML[51] Working group of the Web3D consotium for the representation of geographical data with *Virtual Reality Modelling Language* VRML[52].

J2ME Location API

First, the *Java 2 Mobile Edition* is one specification next to the so called Java Standard Edition (SE) and the Java Enterprise Edition (EE). Two different configurations can be distinguished. The first one is the so called Connected Limited Device Configuration (CLDC) and represents the minimum needed to operate the Java virtual machine. The implementation of a demonstrator as described in section 6 (p. 149) is based on this configuration which is available on almost any mobile phone. The second configuration is the so called Connected Device Configuration (CDC) and is a subset of the Java SE.

The J2ME Location API [102] is an optional package that aims at enabling device independent access to location specific functions of mobile devices. The received geographic location and orientation information can be further used by the J2ME application logic. In section 6 (p. 149) shows a J2ME application which indeed uses location information provided by the network operator but could be extended to use the J2ME Location API.

[44] fring: http://www.fring.com/ (last viewed 6. Jun. 2009)
[45] IERS: http://www.iers.org/ (last viewed 1. Mar. 2009)
[46] GSDI http://www.gsdi.org/ (last viewed 2. Mar. 2009)
[47] G-XML: http://www.dpc.jipdec.or.jp/gxml/ (last viewed 1. Mar. 2009)
[48] ISO/TC 211: http://www.isotc211.org/ (last viewed 1. Mar. 2009)
[49] ESDIS: http://esdis.eosdis.nasa.gov/ (last viewed 1. Mar. 2009)
[50] OGC: http://www.opengeospatial.org/ (last viewed 1. Mar. 2009)
[51] GeoVRML: http://www.ai.sri.com/geovrml/ (last viewed 1. Mar. 2009)
[52] VRML: http://www.w3.org/MarkUp/VRML/ (last viewed 1. Mar. 2009)

SIP (Session Initiation Protocol)

As the name SIP [103] implies, its aim is to allow for the signaling and management of internet based telephony. It is developed by the IESG (Internet Engineering Steering Group) group which is part of the IETF (Internet Engineering Task Force) that is a coalition if industry and research institutions.

SIP is an application-layer protocol and is based on HTTP. It main purpose is to control sessions of applications that exchange or distribute multimedia content. Furthermore, due to its independence of lower-layer protocols and its modular design it is a basic module of future networks like the IMS (IP Multimedia Subsystem) [104, 105] where it is primarily applied for the realization of authentication and charging of users, session management and Quality of Service (QoS).

Apart from the manifold applications that already make use of SIP, new promising approaches such the one proposed by M. Happenhofer et al. [106] that make use of IMS for authentication in order to manage HTTP sessions within a SIP dialog. This not only allows for the development of novel, web-based applications but also overcomes the lack of IMS terminals that is still crucial for the delay of the IMS/NGN rollout.

Mobile Location Protocol (MLP)

The Mobile Location Protocol V3.1 (MLP) [107] is specified by the Open Mobile Alliance (OMA) (see below) and describes an implementation-idependent application-level protocol and at the same time specifies the interface between the network operators Location Server and the client that request location information. MLP does not prescribe which protocol to use, nor is its use limited to certain clients. This means that it can be implemented on almost any mobile device such as mobile phones, personal digital assistants or others, as long as they have access to a network.

The Open Mobile Alliance (OMA)

The document [108] delivers technical specifications and functions for the use of geo information services and map solutions on application level and service frameworks.

Internet Engineering Task Force (IETF)

The IETF is an open standards organization that specifies protocols for integration of location information with internet and web-based applications [109]. Gruteser and Grunwald [110] mention that the IETF Geopriv working group [111] concentrates on the design of protocols and APIs which shall allow the transfer of high resolution location information to external services in a confidential and integrity-preserving manner. Location server are capable of adapting the resolution of location information according to the subject's policies and provide means that allow to transform location information from one format to others. Regarding the exchange of location information they also keep an eye on the secure transfer of location information from and to location servers by the use of pseudonyms.

Open GIS Consortium (OGC)

The Open Geospatial Consortium[53] leads the development of standards for geospatial and location based services. It comprises more than 220 companies, government agencies and universities particu and on a voluntary consensus. Amongst many other standards accessible on their website the also specify the interfaces and interoperability of *OpenLS* which is used for a wide range of different applications[54]

2.4.4 Privacy Concepts

Privacy is one of the human rights and also there the definition is not absolute but varies depending on different aspects such as the context and environment. In this respect *The Public Voice* [112] which was established in 1996 by *Electronic Privacy Information Centre* [113] mentions one writer's statement *"in one sense, all human rights are aspects of the right to privacy"*.

Meanwhile *the Public Voice* identifies four different privacy concepts which include[55]:

- *Information Privacy*: Alan F. Westins definition of privacy [86] at the beginning of this chapter is often referred to as *information privacy* and regards all means that are necessary to provide rules that govern the collection and handling of personal data[56] also referred as *sensitive personal data* by the Data Protection Act 1998 [114]. It includes credit information, medical and government records as well as racial or ethnic origin, political opinions and religious believes to name only a few. The sum of all these rules and activities is also known as *data protection*.

- *Bodily Privacy* concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches

- *Privacy of Communication* covers the security and privacy of mail, telephones, e-mail and other forms of communication and

- *Territorial Privacy* which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

Information privacy is with regard to computer-related privacy issues probably the most important one of the four privacy concepts. Thus in the following we continue with a more detailed discussion about three aspects on information privacy that are *Controlled Disclosure*, *Sensitive Data* and *Affected Subject*. The aspects of information privacy are also discussed in Pfleeger [87] (p. 604).

Social platforms reveal the problem of how to control private data once it is disclosed.

[53] OGC: http://www.opengeospatial.org (last viewed 1. Mar. 2009)

[54] Applications using OpenLS: http://webmap.geoinform.fh-mainz.de/okgis/ (last viewed 1. Mar. 2009), http://www.heidelberg-3d.de (last viewed 1. Mar. 2009), http://www.rewob.de/ (last viewed 5. Jul. 2009)

[55] The privacy concepts are also referred by "A Privacy Snapshot": http://www.ombudsman.mb.ca/reports/snapshot.htm (last viewed 1. Mar. 2009)

[56] Definition of Personal Data: http://www.sussex.ac.uk/records/1-2-11-1.html (last viewed 1. Mar. 2009)

There is no question about someone's *right* to control over the information he reveals about himself. This includes information that affects almost any aspect of life and is strongly related to term *Sensitive Data* which is discussed in the next section. But, what about data that is revealed carelessly. Does anyone who knows about the pitfalls in the web really reveal his private data carelessly? Obviously, there is not the talk of suspicious websites nobody would give his credit-card number to or enter any personal data without somebody's thinking. The problem is rather that many people, including careful ones who take care not to reveal too much information about themself, do not consider that they also give away a bit of their privacy, for example when they participate in customer loyalty programs of supermarkets or airlines. Since such programs have become common practice it is of course difficult or even impossible to avoid services that require some personal data. And it is not a new invention of the internet that personal data is also required for the exchange goods and services. Like in communications, at least some identifying information is always necessary.

But what is then the real trouble with all the services in the web, loyalty programs and the collection of private data? Certainly, one is the booming variety and multiplicity of services which makes it difficult to keep track of every transaction. In this regard we do not only mean online services but any service that collects and uses personal data. By way of comparison, mobile network operators meanwhile avoid to send a monthly paper based phone bill that usually contains a long list of every call and service request. To spare cost, the list can be downloaded by the customers themselves. Similarly, most people do not track every financial transaction of their home bank because it is a time consuming and for most an annoying task. Even though many users are unconcerned or simply uninformed about the data traces they leave one should not ignore the fact that this data is still collected, stored and processed.

One alarming result that arises from the users lack of knowledge or interest about what is already known about them is the agreement to oppressive contracts. Therewith users are not only unable or have difficulty to control their remotely stored data but additionally they loose further control in a sense that they have difficulties to contract out of agreements within the period agreed.

The introductory example of this chapter about vile practices of social platforms with regard to collection, disclosure and processing of private profiles clearly shows that the careless dealing with private data is not an exception but rather a concomitant phenomenon of these booming platforms. Social platforms have probably the most immediate and far-reaching consequences concerning the control and disclosure of privacy sensitive data. The combination of having no direct influence on what is done with personal data by others (friends, operators, companies) now, and how information that is revealed today influences the professional or private life of persons in the long-term is not clear. It is however obvious that any information that is made accessible to others can also be copied, forwarded and stored for more than a lifetime. Private information that is shared between friends from face to face is hopefully treated confidential if the confidant exercises discretion. In contrast to that, once personal information is conveyed and accessible in electronic form it is almost impossible to exercise full control.

2.4.5 Sensitive Data

Apart from the question what mechanisms have to be provided to guarantee privacy and what the reasons are why people continue to reveal private data in the knowledge that they give up a bit of their privacy, we discuss the next question what sensitive information actually is. From a broader point of view, there are private and also cultural aspects to consider and these may vary from case to case. For example, depending on the actual situation one may decide whether to betray the name of someone other or not. In general, information may be classified as sensitive in one case or situation but not in another. Even a decision made now may influence what is considered to be sensitive data later. The following discussion about sensitive data mainly refers to communications and network operators infrastructures.

Traffic Data

In order to be able to transmit content data every modern communication system also requires and generates *traffic data*. As this kind of data directs content from a sender to the receiver it enables communication at all. Every written letter requires an address written on the envelope to deliver the mail. Also electronic mail requires an email address to deliver the content to the respective mail server. In modern telecommunication systems traffic data, also termed as *signaling-data*, contains much more than just the return address. It comprises all data that is necessary to control communications in a telecommunications network. This includes the establishment and control of a communication connection, session and the management thereof. Thus, a signal is used to inform the receiver that a message is to be sent [115]. Section 2.4 (p. 47) discusses legal issues referring to *traffic data* and *locaiton data*. In the next section we discuss *location data* from a network operators point of view.

Location Data

In mobile networks a subcategory of the previously discussed *traffic data* or *signalling data* is *location data* of mobile users. This information is indispensable information for the operation of today's mobile networks. Every mobile device that connects to a network first determines the base station of which the received signal strength is the best and connects to it. Together with the International Mobile Subscriber Identity (IMSI), the Temporary Mobile Subscriber Identity (TMSI), the serial number of the mobile phone, the current location information of the mobile is transmitted to and stored by two central databases that are at the core of each network operator, namely, Home Location Register (HLR) and Visited Location Register (VLR).

One function that is inherently important for the operation of mobile networks is the *location update*. It is necessary to establish telephone or data connections. There are basically two kinds of location updates, *periodic location update* and *initiated location update*. Further details of these operations are described in section 2.2.3 (p. 16).

2.4.6 Movement- and Transaction Privacy

Generally, no-one should be able to track my movement without permission. The use of location-based services shall allow mobile customers to authorize who may access actual lo-

cation data and, depending on the respective application at hand, if also access to movement data shall be prohibited or not. This is relevant for tracking applications where it is essential not only to protect the actual position but also the movement profile.

Transaction Privacy is strongly related to identity privacy and also to location and movement privacy. The reason is that if information about movements is available, this may divulge transaction information through correlation with information of other entities [116].

2.4.7 Management of Privacy Sensitive Data

One example that clearly shows that the management of privacy sensitive data plays an important role for the society is the introduction of the electronic health record (EHR) [117]. This helps to reduce the increasing costs that put the health care system under pressure and by the same token improves the quality of services offered to the patients. Robust and reliable pseudonymization techniques are required that on the one hand securely store anamnesis data to prevent from unauthorized access and on the other hand allow just-in-time access to emergency data that is a special subset of medical data, in emergency cases.

Systems and architectures such as those proposed by Riedl et al. [118] can guarantee the privacy of electronic health records by applying concepts of data sharing, authorization and data recovery in a way that access to privacy sensitive data is under the strict control of the patient and can be restored even in case the patients' security tokens are lost. Furthermore, in [119] develop a variation of the pseudonym based access scheme that is proposed in this dissertation (see Section 4.2 (p. 97)) and which allows just-in-time access to emergency data that is a subset of the stored medical-data.

2.4.8 Privacy and Mobile Phones

Identity- and Location privacy is one of the key issues mobile operators have to face. Theft or loss of mobile devices may reveal much of the users personal information. Different personal data such as address book entries, emails and short messages, pictures, voice records and the call history are sensitive information that reveal much about the owner of the mobile phone. The current development trend shows that in the near future mobile devices become even more ubiquitous. Future mobile devices and applications will be able to assist us in every-day situations, allowing us to access personal and public data and resouces "anytime, anywhere" [26] (page 1). Apparently, future mobile devices seem to be all-rounder with easy access to the internet and hence access to computing power that was never before possible at such low prices. Roughly speaking, during the last 10 years mobile devices rapidly developed from clumpy wireless phones to full fledged mobile computing platforms that are capable to communicate with other devices or access services in a way that was, at least untill recently, reserved to personal computers or, in more general terms, rather stationary computers only.

However, apart from the positive effects of this development this also introduces the whole doom of attacks that is commonly known from the internet. The multitude of communication capabilities which is today a crucial success factor for the viability of mobile makes them also vulnerable to an unmanageable number of various kinds of attacks. At the moment there are no real viruses seen that may harm mobile devices except for some trojans such as Skulls.A[57]

[57] Skulls.A: http://www.f-secure.com/v-descs/skulls.shtml (last viewed 6. Jul. 2009)

and its variations or Commwarror[58] which distributes itself self-dependently over Bluetooth or MMS to name only a few. Other trojans and viruses are can be classified as rather artificial and the demonstration of the possibility of viruses for mobile devices was often rather fear-mongering. The remaining results of these prototypes of trojans and viruses showed that under certain circumstances it is possible to achieve almost the same results as with potential real viruses. This development should not be unnoticed.

Future viruses for mobile devices with the same destructive potential as the already existing ones do probably not have to be expected in the near future. But, spam for mobile devices is another much more realistic thread that is likely to become reality in the near. Mobile users are already confronted with advertising messages, mostly sent out from their mobile network operator and that can just barely be tolerated [68]. Similarly, any kind of location-based advertising is known to be perceived as intrusive and should be avoided. But, apart from advertising messages also real spam received by mobile users is already the reality.

The situation becomes even worse since serious contributions from the academic allows no denying that the thread may become even worse in the sense that during the next years re-programmed bot nets will not just initiate spam emails but also Voice over IP (VoIP) calls. Provisions against this new thread *SPam over Internet Telephony* which is also known as SPIT are much more difficult to develop since SPIT prevention requires different methods than those used for email spam. Moreover, today research in SPIT prevention is in the fledging stages [120, 121].

Protection of Personal Data

Another important aspect that has to be considered with respect to privacy and mobile phones is the mobile network system itself. As a result of the above discussion about the mobile devices and their many different communication capabilities which opens the floodgates for threads it can be said that most of these attacks cannot be prevented by the network operator per se. In other words, the network operator cannot be blamed in case a customers' phone is hacked and some important data is stolen.

One example is Bluetooth that is an industrial specification for the creation and communication within wireless, short range personal area networks (PANs). Meanwhile almost any mobile devices implements Bluetooth which allows the establishment of wireless communication links. Whereas the implementation of the bluetooth stack and hence the bluetooth communication is correct and secure by itself, the most dangerous security vulnerabilities are caused by the different implementations for mobile devices. However, once a vulnerability is detected it can simply be fixed with firmware updates. Well known implementation dependent attacks are *BlueSnarf* [122], *BlueBug*, *HeloMoto* and *Blooover* [123]. A good overview about wireless communication and in particular Bluetooth can be found on the website trifinite.org[59] Another kind of vulnerability is related to the Bluetooth protocol. As such, the protocol is secure and there are no known flaws, it is anyhow vulnerable to certain attacks. Examples are *Bluejacking*, *Pin Cracking*, *Social Engineering Attacks*, *Range Extension*, *Movement tracking*, *Blueprinting*, *Finding non-discoverable devices*. To prevent from such attacks changes of the Bluetooth standard would be required. As Petraschek states in [123], countermeasures against

[58] Commwarrior: http://www.f-secure.com/v-descs/commwarrior.shtml (last viewed 6. Jul. 2009)
[59] trifinite.org: http://trifinite.org (last viewed 6. Jul. 2009)

e.g. Pin Cracking are technically possible whereas in case of Social Engineering Attacks the users have to be sensible of possible attacks when pairing with unknown devices.

Protection of private data stored on mobile devices such as address book entries and configurations as well as all kinds of near field communication capabilities such as Bluetooth may provide vulnerabilities that can be exploited by an attacker. As already discussed, for the protection of this kind of data the network operator is not responsible. However, there is also privacy sensitive data that is network specific. For this kind of data network operators have to provide appropriate measures to avoid that such network specific data that is generated, stored and processed within the network, that is furthermore essential for the operation of the network, is not accessible by non-authorized.

As discussed in section 2.4.5 (p. 58) the importance and the meaning of *Location Data* from a network operators point of view is evident. This clearly shows that location information and in particular *location data* of each particular mobile user is one of the main system-internal functions of every mobile network operator. Without this knowledge, mobile network operators would not even be able to provide telephony and data services at all.

The current location of users is network intrinsic and thus as such not accessible from outside. However, information such as the *Cell-ID* that indicates a particular base station and the *location area code* (LAC) can be accessed with little effort and there are many possible ways to achieve this[60]. The customers current location is one of the most prominent examples that shows how privacy sensitive information is generated and processed by network operator. There is no doubt, that in general *traffic data* which also subsumes location data has to be protected by the network. In this respect also legal requirements and obligations that aim to protect sensitive information about the customers play an important role. We discuss this issue is discussed in section 2.4 (p. 47) in closer detail.

Even though location information is important and as such has a special characteristic regarding the users location privacy, there are also a number of other network specific aspects that have to be considered which we discuss in the following section.

2.4.9 Vulnerabilities of Mobile Networks

Operators are certainly aware of one of the biggest assets that is the customers confidence that they handle their sensitive data in a confidential manner. This includes all technical and organizational means in accordance to legal obligations and requirements. In [124] K. Rognsvåg tells his favorite story that shows the importance of privacy protection and what consequences the disregard of proper measures may have. The story describes a how a customer receives messages from other furious customers just because of an error in the telecom system. A MMS that contains a picture of the customers 'private parts' and that was intended for his girlfriend only but sent to hundreds of other customers due to an error. Errors like these certainly raise unpleasant questions.

There are obviously some other frequently asked questions that clearly address some of the core functions of mobile networks and indicate that there is an apparent public interest in the security of networks and the handling of personal data. Questions regarding the technical

[60] Symbian Programming: http://mikie.iki.fi/symbian/ (last viewed 6. Jul. 2009)

details about the possibilities of network operators such as how to locate or monitor users are indeed most widely unknown to the public. As for many cases it is understandable and makes even sense that operators keep the details secret. However, there are a number of security weaknesses that arise from the deployed standards and that partly explain the frequently asked questions published by the *Federal Office for Information Security* (BSI)[61] on mobile communications:

Is it possible to localize or activate even switched off mobiles? Only if any manipulation of the mobile devices can be excluded it is not possible to identify the position of a switched off mobile phone. Similarly, mobile devices cannot be activated as long as they are switched off which would enable eavesdropping conversations. There are only two possible cases when such attacks are achievable. First, an attacker manipulates the mobile phones hardware or firmware. Second, the attacker exploits detects and exploits hardware or firmware errors.

In any case the BSI advises not to use mobile phones with uncertain origin as presents and leaving the phone unwatched for a longer period.

Is it possible to manipulate software via air-link? It can be assumed that most mobile devices already contain software modules that can be used to insert other malicious software modules (e.g. during service) and thus allow to listen into rooms without unbeknownst to the owner. Such brought in software modules could in the near future be activated via air-link. Especially phones that provide SIM-Toolkit capabilities such as they are expected to be distributed in future and be used for mobile banking could be abused through transmission of special SMS commands. It is further expected that in future unified mobile hardware platforms allow software updates even across different networks. This may also introduce attackers to possibly insert malicious software. Given that, to prevent from attacks, manufacturers are required to distribute only encrypted software.

Is it possible to make mobile phones inviolable? There are no means that allow to proceed from total security. There are different possible ways to enhance security and to prevent from some of the previously mentioned threats. As some of these threads stem from the network operators infrastructure, some additional measures such as mutual authentication between the mobile phone and the base station, end-to-end encryption even over different network operators domains right up to the realization of a special mobile phone with dedicated security features aimed for high level security demands.

Obviously, no matter what kind of thread has to be expected in future, any kind of attack, including the examples described above, may stem a harassment for the mobile industry and at last severely violate the privacy of mobile users. In the light of the possible scenarios and expectations for the future, users are well-advised to not accept mobiles from unknown sources, pay attention on their own mobiles to that it does not get lost. Of course, it is difficult to always pay attention to the mobile phone and there are certain cases where the malicious use of software and services is difficult to prevent or detect. In section 2.4.2 (p. 52) we already mentioned legal requirements in Europe

[61] BSI: http://www.bsi.de/faq/mobilfunk.htm (last viewed 6. Jul. 2009)

that aim to prevent from cases such as those that enables users to retrieve the location information of other users without their knowledge or consent. Dedicated measures that prevent from such malicious use of software and services are required. Both, network operators and services providers are constrained to provide the appropriate measures.

Mobile network operators are aware of the importance of the sensitive data they deal with. Anyhow, it is difficult or rather impossible to completely rule out the possibility that some errors occur. It is the operators obligation to provide proper means that keep the security level high. But, as consequentially states, security does not give privacy, even though security is a prerequisite to privacy [124] (p. 28).

2.4.10 Location Privacy

Location privacy as a subcategory of *information privacy* and can definitely be referred to be the most important privacy aspect with respect to location-awareness and location-based services [69] (p. 34). According to Alan Westins general definition of privacy, location privacy is the claim of individuals to, shortly spoken, have their location information under control. Location Privacy has also become a key issue in the area of pervasive computing research [45] In this regard, location-awareness as a special type of *context-awareness* also concerns the minimal set of necessary contexts that are denoted as the five "W"s which are mentioned at the beginning of chapter 2.1 (p. 5) Context-Aware Computing. The third "W" which stands for "Where?" can be interpreted as the representative for all the necessary capabilities to sense a person's location which at large composes the location-aware computing environment. Even though *location privacy* narrows down the general notion of *privacy* and *information privacy*, it still provides diversity in interpretation and definition. One such definition is given by Beresford and Stanjano: "*the ability to prevent other parties from learning one's current or past location*" which in essence should bring people under control of their location information [125]. The users ability to determine who may access location information right now is only one side of the coin. The definition given by Beresford and Stajano also refers to location information of the past. Similar to web servers, also location servers log every request and location information that is either received from mobile users equipped with GPS devices or location information that is associated with cell-IDs provided by the network operators. These basic functions like reading and writing and additional services that run in the background such as logging are obviously similar to those provided by web servers and there is no question that during service operation large amounts of location data accumulate in logs, similar to web servers log entries of each and every request. Location-based service providers without malicious intentions that provide means for privacy protection and furthermore adhere to high security standards for service access by anonymizing location logs may anyhow provide enough information for inference attacks that join several sources of information and finally reveal the identity of individuals. As a result, legal edicts may even oblige operators to provide release recorded traces of individuals, affirmed by legal edicts and used for criminal prosecution (Gruteser and Grunwald [110]).

For many people, understanding their privacy sensitive data in general and their whereabouts in particular is new and difficult. One reason for that is that many location-based services and applications do not provide appropriate means that allow users to be in control of with whom and to what extend they share privacy sensitive information, in particular

location information. And if it did, the systems mostly provide only rudimentary means of control. Anyhow, the widespread use of navigation systems fosters the use and adoption of location information in every-day life. Since most of these applications do not necessitate the exchange of location information with other services or persons, there is no incentive to raise the awareness of the importance of location information or being in charge of control of it.

One project that aims to raise awareness of the user's privacy sensitive location information is POLS (Privacy-Observant Location System)[62]. Differently, the system does not require to contact any service provider nor any network operator to determine the actual location. By using the POLS application, the mobile device listens for nearby radios of GSM cells and WiFi access points and uses the received unique IDs to for the estimation of the actual position. The received IDs are then further used to request the precise position from an internal database [126]. The idea to provide move the location information that corresponds to certain unique IDs to the client allows to determine the actual position without leaving any traces on servers that may perhaps later be used by malicious intruders. Despite its simplicity this solution has the obvious disadvantage, that the position information is still not available in requested quantity. At the time of writing this dissertation only the Seattle Metro area is available[63]. But, the POLS project also offers two additional applications called *POLS stumbler* and *Log Cooker* for building own beakon maps or mapper files.

Duckham et al. [45] conclude in their publication in section *the right to location privacy* that due to the fast development of technology that allows for more reliable and precise localization technology, location privacy is on the one hand likely to amplify location-privacy concerns. On the other hand, the awaited success and acceptance and uptake of location-based services highly depends on the quality of the applied privacy protection mechanism. Location privacy can thus already be identified as key research question for the development of location-based services and generally in the research field of location-aware computing. Finally, location privacy has become an key issue for pervasive computing research.

2.4.11 Threats Resulting from the Availability of Location Information

With the advent of various new kinds of location-based services it is obvious that location privacy will in future play an important role for all parties concerned. But, aside from the regular questions how location privacy can be actively achieved, that means the secure exchange of location data from one entity to another, the analysis of location privacy reveals that this is associated with identity privacy [116]. Knowledge about the position of a certain entity gains much more value if it is not the question of someone anonymous but an identified entity.

What are the main reasons for privacy threats? Because location-based applications mainly rely on the implicit assumption that users agree to trade their location privacy by the service the only way to keep location information private would be to stop sending further location information or to temporarily unsubscribe from the location-based service. As this is practically impossible it is vital to provide appropriate means that guarantee location privacy and at the same time protect the user's identity.

[62] POLS http://pols.sourceforge.net/ (last viewed 21. February 2009)

[63] Seattle Metro area: http://pols.sourceforge.net/img/coverage_map_20051121.png (last viewed 1. Mar. 2009)

So far, the dissemination of location-based services introduces different kinds of threats that clearly show the importance of protecting privacy as a whole. There are at least three well known possible negative effects that may occur if protection of location privacy fails. Duckham et al. [45] mentions these which include:

- *Location-Based spam*: Convey of unsolicited advertisement based on the users location.
- *Personal wellbeing and safety*: The most prominent example here is that of stalking. Through unauthorized or unrestricted access to location information users may be exposed to various forms of dangers that range from tout and stalking right up to physical threats.
- *Intrusive inferences*: Since our sphere of action is determined and simultaneously constrained by location this allows also to infer personal information of other users.

As the last point suggests, an important aspect of location privacy is the distinction between location information that is received in real-time and previously recorded location tracks, as such, the difference between location information that is generated and captured while in transit and recorded location information. The latter one can further be divided into single location points that are buffered and released with only a short delay and complete GPX tracks of users collected even over longer time periods.

Long-term records of tracks are analyzed by Gonzlez et al. [127]. Their findings of mobility patterns of mobile phone users reveal interesting insights that are highly significant for a better understanding of basic laws governing human motions. Their analysis on movement patterns identify temporal and spacial regularities in human movements which show that people follow simple reproducible patterns. We can confirm this since after we have collected only some dozens of GPS tracks for our tracking platform we recognized that most tracks were equal. Similarly, if some users ask for the next pizza restaurant to their home, they may reveal their true identity based on the location if the traditional approach of pseudonymity, that is using fake identities, is used [128]. This interesting insight also serves as prerequisite for the development of applications in different domains.

John Krumm [125] (p. 3) concerns attackers gaining access to location data and using it to algorithmically discover a subject's whereabouts and activities. His survey gives a good overview about privacy mechanisms and discusses studies on peoples' attitudes about location privacy as well as threats and countermeasures. Furtermore, he shows that stored location traces can be used to identify significant locations such as the home or workplace of users. He refers to early work on the analysis of movement such as those proposed by Marmasse and Schmandt which allows to identify significant places where the GPS signal is lost three or more times within a predefined radius [33] and their subsequent work where combinations of the dwell time, breaks in time, distances and periods of low GPS accuracy are used [129].

Inference Attacks on Location Tracks

In the paper [125] Krumm further mentions four noticeable reported studies on privacy attacks by Beresford and Stajano [73], Hoh et al. [130] (GPS traces from 239 drivers in Detroit), Krumm [131] (this paper is discussed below) and Grueser and Hoh [132] (use of completely

anonymized GPS data, even without pseudonyms). All attacks described here are generally referred as so called *inference attacks*. This kind of attacks operates on stored and pseudomized location data. It can be shown that it is possible to not only identify significant locations but also the home locations of individuals and and even their identities.

At the time of writing this dissertation, J. Krumm himself denotes in the paper *Inference Attacks on Location Tracks* [131] that so far there are no other known perceptions on computational inference attacks on recorded GPS data as well as no assessments on the effectiveness of certain countermeasures. In this context he further tests three countermeasures *Spacial Cloaking*, *Noise* and *Rounding*. This allows to determine how much location data needs to be cloaked, faded away or rounded in order to be able to best possibly protect the individuals home address location. First, Krumm shows that out of 172 pseudonymous GPS tracks those users' home location with a home location median error of 60 meters are identifiable. Given these locations it is in turn possible to identify the name of 5% with web-based white pages lookups. The following three countermeasures that are applied to the raw GPS data shall prevent from *inference attacks* [131]:

Spacial Cloaking Different to other spatial cloaking concepts such as *k-anonymity* [133] This approach operates on data of single persons instead of groups of people that are in the same region. Four algorithms were tested for *Spatial Cloaking*: Last Destination (best-performing), Weighted Median, Largest Cluster, Best Time.

Noise is another possible way to prevent from inference attacks. Except for noise that arises accidentally and that is attributable to technological effects or other inevitable influences, noise may also be produced intentionally. Krumm refers to Agrawal and Srikant who describe in [134] the process of returning $x_i + r$ instead of x_i "*value distortion*" where the value of r is a random number and subject to any distribution.

Rounding is termed by [134] as "*Value-Class Membership*". Here, the location data is assigned to different dedicated disjoint classes and only the information about the class which the actual location corresponds to is returned.

Identification of Future Location Tracks

Other attacks aim to find out future tracks of users. If an adversary could reveal the identity of some individuals it is easy to predict when and where some individuals will go to. In this case the adversary can even shadow individuals. The more information and adversary collects the better the predictions are. Finally, an adversary may have collected enough information to build a complete picture of each movement of both, the past and even the future.

In [125] Krumm mentions Beresford and Stajano [73] who introduce entropy as privacy quantifier and show that behavioral probabilities as they can be expected for e.g. a u-turn can be linked to changing pseudonyms.

The most prominent context-aware variable is the one that describes the location of objects or subjects. In telecommunication systems, location information is generated and processed by and within the network (see section 2.2.5 p. 19). Location data belongs, amongst others, to the so called *signalling data* which is primarily necessary for establishment of phone calls.

Apart from the technical questions, how location data is generated and processed, *Location Data* and *Mobile Positioning Techniques* as well as the protection of the location of individuals and finally the aim to achieve location privacy is a very complex matter. There are also many non-technical questions that rather focus on social and legal issues. Since it is not possible to foresee many of the problems that may occur in specific systems, the results from user studies and research that investigates the underlying motivations and behavior patterns of users provide a viable input even before location-based systems an applications are build. In the following we consider questions such as how user preferences may be controlled by the users themselves while sharing location information with others and what means have to be provided to allow this.

2.4.12 Privacy Management

In [135] Mika Raento and Antti Oulasvirta present the idea of privacy *management* which has, as they note, its roots in various disciplines including ethics, social psychology, law and computing. The design and implementation of the corresponding social awareness service is discussed in detail in [14]. They hold the view that privacy management is a process by which individuals relocate their self-environment boundary according to their actual needs as part of a negotiation process. We will discuss a basic concept and implementation of such a negotiation process in section 7 (p. 160). According to M. Raento et al. [135] (p. 2) privacy management can be seen as the collection of a number of constituents including:

Control means that the type and amount of the exchanged information is defined in advance and may change according to the changing environment and in due consideration with the actual users' needs and preferences.

Accountability relates to the fact that every time information is disclosed it is up to the receiver to stick to the agreed arrangements.

Plausible deniability allows users to appear as *unavailable* or to not transmit or allow access to her location information. Being randomly unavailable could also be implemented as a privacy feature, although it would rather be attributed as a bug of the system. In any case and any form of implementation, systems that provide a way for plausible deniability relieve users from the burden to explain why they were not visible or available [128] (p. 52).

Reciprocity of data means that one cannot receive data from others unless she is also sending her data whereas reciprocity of interaction means that by accessing someones data this person is instantly informed about who is granted access which prevents from unwanted observability [128] (p. 52).

Utility of private data is certainly difficult to measure, if it is measurable at all. Usability tests undertaken by N. Marmasse [129] investigating the utility of communication with a communication tool in form of a watch (*WatchMe*) as basis to see the utility of the exchanged context information in case any modality was chosen for the conveyance of information from one person to another.

2.4.13 Privacy Models for Protection of Location Information

The design and implementation of systems that process context-information and in particular location information is, as already mentioned before, a difficult task which depends on various partially varying factors. One of the key concerns is the protection of the users' location information. Therefore, appropriate privacy models shall be applied which mainly cover the imperfection of spacial information.

Three types of *imperfection in spatial* information are listed by M. Duckham and L. Kulik in [45] and commonly identified in the respective literature:

inaccuracy describes the fact that some information is not correspondent to reality. In other words, systems that make use of this type of imperfection of spacial location information need to lie about about the users' locations.

imprecision is often confused with inaccuracy as some expressions describe facts and circumstances more accurately but less precise. Thus, *accuracy* and *precision* are orthogonal to each other. The use of imprecision for obfuscating locations provides many advantages. Shortly spoken, the advantages include flexibility, obviation of high level policies, revelation of the users' identity and protection against data mining offensives.

vagueness depends on boundary locations which cannot be assigned precisely as being within or not within certain well-defined areas, near or not near, and so on.

M. F. Mokbel [128], (p. 3) differentiates three paradigms:

The minimal information sharing paradigm proposed by R. Agrawal [136] results from research in the area of databases, in particular intersection and join operations among databases using cryptographic operations for encryption and decryption without the need of third parties. It accommodates the need of revealing not more information among other databases and systems than necessary. The reasons are e.g. the integration of information systems for the realization of e-business scenarios, outsourcing and cooperative activities among companies as well as security and privacy requirements that are triggered by governmental and privacy legislation regulating privacy policies on information sharing.

The untrusted third party paradigm is realized by a system that is proposed by F. Emekci et al. [137]. It is a hash based peer-to-peer system that allows for anonymous and secure communication and computation. It allows to select third parties that take over the part of computation for the privacy preserving queries. These queries are executed over multiple providers' data.

The trusted third party paradigm is perhaps the most commonly used. Here, one or several server act as intermediary between users and service providers. Anonymizing service like *Tor* [138] or the online payment service *PayPal*[64] are indeed diverse in their application but follow the same concept.

[64]PayPal URL: https://www.paypal.com (last viewed 21. Feb. 2009)

Mokbel [128] further lists four different approaches that aim at protecting the users' identity while updating its location information on a location-based service.

False dummies : the users send not only one but n different locations as part of a location update message. This simple location update strategy hides the true location of the user but also generates more data traffic.

Another approach that aims at increasing location privacy but has similar side effects such as more generated traffic is the use of *dummy users*. A. R. Beresford and F. Stajano [73] discuss this strategy in the light of further research directions on location privacy and the use of their proposed mix networks. They conclude, that the concept of dummy users is difficult to realize especially in the pervasive computing environment where dummy users need to fulfill even complex real-world tasks.

Landmark objects : in this case not the exact location but the location of some significant nearby object or landmark is sent. The *Confab* system by Hong et al. [139] makes use of this location scheme.

Location perturbation : this method distinguishes two kinds of *blurring*. One way is spatio-temporal cloaking where not the exact location information is sent but only a spatial region. Concepts like k-anonymity which is discussed in section 2.4.16 (p. 70) or graph models can be applied here. Another method is *obfuscation* of location information (Kuliks formal model of obfuscation cited) In both cases the blurred but not the exact location is sent.

Avoid location tracking : users hide their location as long as they are within sensitive regions.

Mokbel [128] identifies three major research directions that aim to protect location information: *pseudonymization*, *location blurring/cloacking* and *policies*. In the survey of computational location privacy J. Krumm [125] cites Duckham and Kulik [69] who also quote these three research directions together with *regulatory strategies* as computational countermeasures for enhancing location privacy. The following discussion elaborates these three strategies but omits regulatory strategies which are discussed separately in section 2.4 (p. 47).

2.4.14 Anonymity and Pseudonymity

J. Al-Muhtadi et al. [140] outline that in general many research activities on privacy and anonymity can basically be classified into *user anonymity* and *anonymous communication*. The first one *anonymity* aims at hiding the users' identity whereas the second *anonymous communication* tries to conceal communication details in order to avoid eavesdroppers learning details about the communication parties.

If we restrict the scope to the needs of location privacy, Duckham et al. [45] and Pfitzmann and Hansen [141] discuss *anonymity and pseudonymity* as to be one possible means to to achieve this. But, a matter-of-fact Duckham et al. state that *anonymity and pseudonymity* cannot provide a complete answer to privacy concerns because *anonymity* can be understood as barrier to authentication and personalization and are furthermore vulnerable to data mining offenses. Relating to data mining, J. Krumm shows in [125] that given only enough anonymous

tracks it is anyhow possible to exactly identify a significant number of persons. We discuss this re-identification in detail in section 2.4.11 (p. 64).

The *"principle of minimal collection"* that is also related to the notion of *obfuscation* which is discussed later assumes the use of only *de-personalized* data for location-based services. Duckham and Kulik [69] mention the work of Gruteser and Grunwald [110] who refer *de-personalized* data as to be *practivally anonymous* data, referring to Pfitzmann and Hansens [141] definitions. Apart from possible attacks such as those shown by J. Krumm, the use of anonymous data provides a number of benefits for service providers and for the users as well. One such benefit is that since the use of anonymous location data, that can be interpreted as *"information that is sufficiently altered to prevent re-identification"* [110] requires no consent of users, the collection, processing and transmission even to untrusted third parties causes in total less overhead.

Examples that make use of means to provide *anonymity* are given by Gruteser and Grunwald in [110] (p. 2). They provide a list of related work which contains among others e.g. *Crowds and Onion Routing* which provides sender anonymity by allowing anonymous usage of services through omitting the users' ID and by solving the network addressing problem. Another example represents the so called *Mist routing project* [140] for mobile users. It represents a combination of location privacy and the use of pseudonyms to achieve *anonymous communication.*

Perhaps one of the most influential work in this area is that of D. L. Chaum [142]. He proposes the fundamental concept of a mix that makes messages untraceable for eavesdroppers and intermediary routers. This is achieved by padding messages to equal size, encryption of incoming and outgoing messages with different keys and prevention of replaying incoming messages. The solution does not require a central authority but nevertheless allows messages to be sent anonymously and as the author concludes *limited anonymity.*

2.4.15 Privacy Policies

The use of privacy policies for location information assumes that users trust to some extend third parties [110] (p. 2). It is necessary to implement unambiguous computer-readable mechanism for location-privacy protection and is undoubtedly a long-term part in the landscape of pervasive computing technology. A drawback of privacy policies is that it provides not a complete solution since policies usually incur considerable information infrastructure overheads and are furthermore vulnerable to inadvertent or malicious disclosure of private information.

Snekkenes [143] proposes location privacy protection by adjusting the precision of location information with policy-based mechanisms. This approach enforces the so called *"need-to-know principle"*. Presuming compliance to this principle, it can be ensured that individuals release only those information that is really needed by a service provider to fulfill requests sufficiently, that is, comply with the information practice principle of consent and limitation. It is further also related to the notion of *obfuscation* which is discussed in the following.

2.4.16 Obfuscation

Duckham et al. [45] define obfuscation as follows: *"...the means of deliberately degrading the quality of information about an individual's location in order to protect that individual's loca-*

tion privacy." As already mentioned in section 2.4.13 (p. 68) the three distinct mechanisms *inaccuracy*, *imprecision* and *vagueness* are crucial for degrading the quality of location information. Duckham et al. [45] use *imprecision* as means for obfuscation in order to protect the individual's location privacy. The reasons are manyfold. One is that obfuscation is flexible which allows to meet certain requirements and contexts. Another important aspect is the compliance with legal requirements that is achieved by jurisdiction aware software [95]. In this spirit obfuscation provides one way to meet not only legal requirements but also obligations set up by some policy infrastructure. Finally, if needed, obfuscation also provides the possibility to disclose the identities of individuals which in turn enables authentication and personalization that is essential for many applications. On the other hand, not revealing the precise location information exacerbates data mining efforts with the aim of revealing the individuals' identity.

Enhancing location privacy of users can also be achieved by lowering the spatial and temporal resolution of location data. Obfuscating or *cloaking* location information means that instead of sending the actual precise location information to a location-based service a user releases only a larger region covered in a time frame. This method has the advantage that users have more control over their own whereabouts accompanied by more location-privacy. The disadvantage of this method is that by reducing the accuracy this also reduces the overall quality of the location-based service [144]. Location-based services that require precise location information are even excluded. Nevertheless, there are also situations where location-based applications operate only on low quality positional information but provide high quality results [69].

k - anonymity

The idea of k-anonymity was first proposed by Sweeney [133] and makes a data attribute indistinguishable with $k-1$ other values. This metric can also be used to provide location privacy. Cheng et al. [144] proposes a metric for measuring the privacy of location cloaking. They also address the issues of inference attacks, where future locations can be inferred based on tracing the movement in the past. They present two approaches, namely *patching*[65] and *delaying*[66], in order to prevent the user's location from being deduced, thereby reducing the impact of this kind of threats.

However, obfuscation, in particular *k-anonymity*, also has some disadvantages which are discussed by Treu and Küpper [145]. One such disadvantage relates to the fact that *k-anonymity* diminishes the location information to an extend that hinders many potential, future location-based services from being operational. Similarly, depending on the current location, be it in rural or in urban areas, localizations that are based on the current Cell-ID may be accurate enough for some applications. This is maybe the most obvious drawback of the *k-anonymity* approach but the following are not of less importance. This approach requires

[65] According to Cheng et al. [144] (p. 410) *patching* refers to a technique that combines past with present cloaked locations. In particular this is done by combining the trajectory of traces which on the one hand indeed reduces the uncertainty of the cloaked locations. But, this is at the same time compensated through the inclusion of the prior cloaked location area which is part completely part of the major dimension of the cloaked area

[66] includes the time aspect which means that requests are suspended for the time till cloaked locations are completely within the maximum major dimension.

a global view on each individual to be able to determine the dynamically changing areas representative for *k-anonymity*. This by itself represents a security risk. Another important fact that has to be considered is the provision of proactive services. If only a single pseudonym is used to veil the identity of individuals the analysis of the history of the covered distances between two *k-anonymous* areas (e.g. workplace and home) allows to unveil the identity with a probability $> p(\frac{1}{k})$.

2.4.17 Identifiers and Pseudonyms

An essential factor for the effectiveness of pseudonyms is unlinkability between the pseudonym and its holder and if pseudonyms can be linked between each other. Pfitzmann *et al.* [141] discriminate different kinds of pseudonyms depending on the following factors:

Knowledge of the linking between a pseudonym and its holder:

Little knowledge of the linking between the pseudonym and its hold provides the highest degree of anonymity. The strength of anonymity decreases the more is known about the pseudonym linking. The scale of anonymity reaches from initially unlinkable pseudonyms on the one side to public pseudonyms on the other.

Linkability due to the use of pseudonyms in different contexts:

More pseudonym uses in different contexts decreases the strength of anonymity. Thus, an increase of anonymity can be achieved if the pseudonyms are changed. In this sense, transaction pseudonym provide the highest degree of anonymity because they are used only once. Beresford *et al.* [73] state, that if pseudoyms are never changed (permanent pseudonyms) de-anonymization is possible with only some available background information about a user.

We make use of permanently changing transaction pseudonyms. This prevents from repeatedly use of equal pseudonyms. Nevertheless, since the mechanism for the generation of such transaction pseudonyms involves a shared secret, each transaction pseudonym can unambiguously be linked to the respective identity. This user defined secret is only known by the user and the privacy service which after receiving a pseudonym may deduce the user's identity. Categorizing the linkage of each pseudonym, only the privacy service is capable of revealing the identity of the respective user. As the privacy service is considered to be trustworthy we can deduce that in our trust model the role of pseudonyms is primarily to anonymize the user's identity towards potentially untrusted 3rd party application provider [9].

Chapter 3

Selected Aspects of Secure Communication

This chapter starts with a brief overview about some of the most important cryptographic ciphers and hash functions that are relevant for this dissertation and continues with the so called Message Authentication Codes (MACs) and the most important security aspects thereof. Message Authentication Codes represent the fundamental mechanism for our pseudonym generation scheme. The discussion is followed by some important cryptographic primitives and services. Since the security service authentication affects our proposed solution most, it is discussed in close detail which includes also its separation from other not less important security services such as identification and confidentiality. We continue our discussion with an illustration of some of the most important authentication schemes which are essential background information with regard to our proposed solution.

3.1 Cryptographic Hash Functions

Today, secure electronic communication is based on cryptographic theory which allows for provable security and is thus an important fundament in cryptographic practice [146]. Be it financial transactions, communication in the military sector or public mobile telecommunications, cryptography affects almost any sector. The exchange of encrypted messages is neither new nor is it an invention our modern society. First known examples when messages were exchanged encrypted go back to ancient times. Not until the invention of transistors which introduced an unprecedented development of computing power many different encryption techniques and schemes have developed. The advent of the internet which further allows utilizing powerful computing resources that are distributed all over the world, a number of algorithms such as the Data Encryption Standard (DES) [147] were rendered insecure. Even though DES was extended several times it was replaced by the Advanced Encryption Standard (AES) [148] which is deemed to be the defacto standard at the moment. Progress in the development of new techniques that allow to break codes, at the first instance at least theoretically and in most cases under the assumption of certain pre-conditions constantly stimulate research in this discipline. For example, the development of the differential crypto analysis which could, among others be used to successfully attack DES in the 1980s was most

likely known already by the designers of DES at IBM in the 1970s. The race between cryptographers and those who try to break ciphertexts and the underlying cryptographic algorithms still lasts and will continue along with the the development of new methods and findings on both sides.

Since this is such an important topic which definitely extends the scope of this work we just omit in the following a detailed discussion and in depth analysis about the various kinds of cryptographic algorithms. For this we refer to Bavaud et al. [149] (p. 254) who, provide a general introduction into cryptography and in addition raise basic questions such as what cryptography deals with. Instead of that we rather concentrate on a dedicated cryptographic class, namely that of cryptographic one-way-hash functions and keyed hash-functions which are both the basis of the proposed scheme used to generate so called pseudonyms. The are at least two reasons why these cryptographic details are important to consider. Firstly, it is important to understand the most general security aspects that are affected by the pseudonym generation scheme. These aspects relate to the security of particular communication parties' roles and secondly explain the functionality of the protocol designed to provide secure communication links between each communication party.

The first row of the following table 3.1 shows two different classic ciphers that are the *Substitution Ciphers* and the *Transposition Ciphers*. Substitution ciphers include e.g. Caesar Cipher or Vigenre Cipher. Whereas these ciphers are based on replacing text, transposition ciphers rather shift positions of characters which corresponds to permutations. The following two rows show some of the most important representative symmetric (DES, IDEA and AES) and asymmetric ciphers. The Diffie-Hellman's key exchange, El Gamal and RSA are perhaps the best known and representatives which are also most used. Elliptic Curve Cryptosystems are not cryptographic algorithms but provide means to on the one hand build cryptographic algorithms which are then on the other hand faster and require shorter keys. The last row provides some cryptographic hash functions. The most prominent ones are MD5, SHA, RIPE-MD and HAVAL. A detailed discussion about each is given in B. Schneier's book [150]. In the following we discuss this kind of cryptographic hash functions in closer detail.

3.1.1 Basic Requirements of Cryptographic Hash Functions

Hash functions are mainly used for establishing data integrity and message authentication. With it, any input of arbitrary length is converted to a string with fixed length. There are two basic properties of hash functions. The first one concerns the compression, that is, the hash function maps some input of arbitrary length to a certain output with fixed length. The second basic property is that given an input it is easy to compute the corresponding hash value. Hash functions correspond to the many-to-one relationship. This means that each of all possible input result in exactly one certain output. This further implies that collisions are unavoidable and raises the question how secure a hash function is. The security of unkeyed hash functions follows general requirements described in [5, 151]:

- *Pre-image Resistance*: given this property and the assumption that it is possible to specify all possible outputs, it is anyhow computational infeasible to find an input which, applied to the hash functions, results in the same output. In other words, given, a secure hash function $h(x) = y$ it is impossible to find the preimage x for a given hash value y.

Classic ciphers	Substitution Cipher (Caesar Cipher, Vigenre Cipher) Transposition Cipher
Symmetric	1976 DES (Data Encryption Standard), 3DES, IBM 1992 IDEA (International Data Encryption Algorithm) Lai and Massey (patent by ASCOM but free for non commercial use PGP) 2000 AES (Advanced Encryption Standard) (Rijndael) Joan Daemen, Vincent Rijmen
Asymmetric	1976 Diffie-Hellmann 1985 El Gamal, Taher Gamal 1977 RSA, Ron Rivest, Adi Shamir, Leonard Adleman Elliptic Curve Cryptosystem
Cryptographic Hash Functions	MD5, SHA, RIPE-MD, HAVAL

Table 3.1: Overview Ciphers and Cryptographic Hash Functions

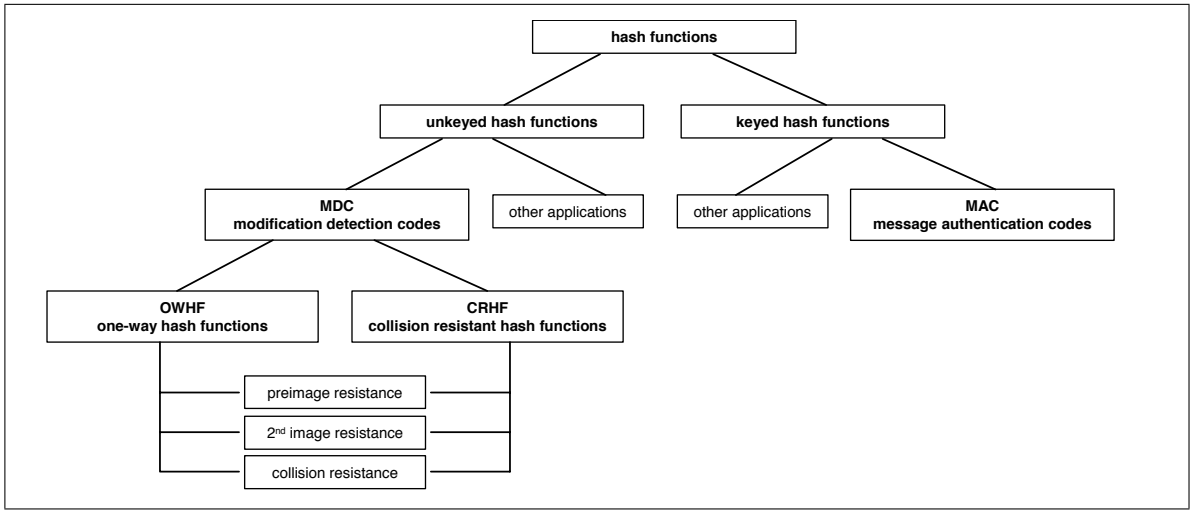

Figure 3.1: Classification Tree of Cryptographic Hash Functions [5]

- *Second Pre-image Resistance*: given any value x_1 it is computationally impossible to find another second pre-image $x_2 \neq x_1$ such that $h(x_1) = h(x_2)$. In other words, for a given output y with m bits, the effort to compute x is on the order of 2^m operations or just as much randomly selected inputs.
- *Collision Resistance*: it is computationally impossible to find a pair of free chosen values x_1 and x_2 such that $h(x_1) = h(x_2)$. In this case only $2^{m/2}$ operations are necessary.

3.1.2 Message Authentication Code (MAC)

Data transmission over insecure communication channels requires means that allow the receiver of messages to validate the authenticity and integrity of the received data. This can be

realized by the use of a Message Authentication Code (MAC). When data is sent from one communication party to another, the sender uses the MAC algorithm to compute an *authentication tag*. The MAC algorithm represents a function of the data and a secret that is shared between the communication parties [152]. Also digital signatures can be used to guarantee message authenticity and integrity. The difference between a digital signature and a MAC is that the former one uses different keys for generation and verification of message signatures whereas MACs rely on a shared key that is only known by the sender and the receiver of a message [1].

3.1.3 Keyed-Message Authentication Code (HMAC)

At the time when HMAC was proposed by Bellare et al. [152] it was indeed clear that a MACs based on a hash function are worth having. By the time before HMAC, most MAC constructions were based on block ciphers like Data Encryption Standard DES [147], the most popular one Cypher Block Chaining Message Authentication Code short CBC MAC. But, there were still unanswered questions such as how to accommodate the notion of secret keys or the missing security analysis. Regarding the properties of MACs Bellare et al. states in [153] (p. 3): "*The properties we require are mainly collision-freeness and some limited unpredictability. What is shown is that if the hash function has these properties the MAC is secure; the* only *way the MAC could fail is if the hash function fails.*" Due to several reasons like export restrictions and performance, MACs were mostly build on hash functions such as MD5 and SHA. Since hash functions are not designed for message authentication per se the question how to use hash functions best was not easily answered for a long time. This changed when the *Hash based Message Authentication Codes* (HMAC) [152, 154, 155] was introduced. It is one step towards a solution to this problem and enables two parties holding a common secret key K to generate a sequence of random numbers.

3.1.4 HMAC operational

The following subsection explains the details of HMAC. The formal explanations are followed by a short discussion about the security of HMAC and its underlying assumptions. In Equation 3.1 the H denotes a hash function. Aside from security considerations, section 3.1.5 explains which hash functions are to be considered best. In general a hash function takes an arbitrary length of bits as input and produces a certain output of l bits such as 128 bits for MD5 or 160 bits for SHA-1. HMAC requires two input parameters. One is a secret key denoted as K which is shared between the sender and the receiver. This key should not be larger than 64 bytes which exactly corresponds to the hashing block. If the key is too long, it can simply be hashed to meet the required length. A longer key makes no sense since it does not increase the security at all. In case the key is too short, the remaining bytes are filled with zeros. The message M is the second input parameter. The HMAC is built up as follows:

$$k = \mathrm{HMAC}_K(X) = \mathrm{H}(K \oplus \mathrm{opad}, \mathrm{H}(K \oplus \mathrm{ipad}, X)), \tag{3.1}$$

[1] RSA Labratories, Crypto FAQ: http://www.rsa.com/rsalabs/node.asp?id=2177
(last viewed 17. Mar. 2009)

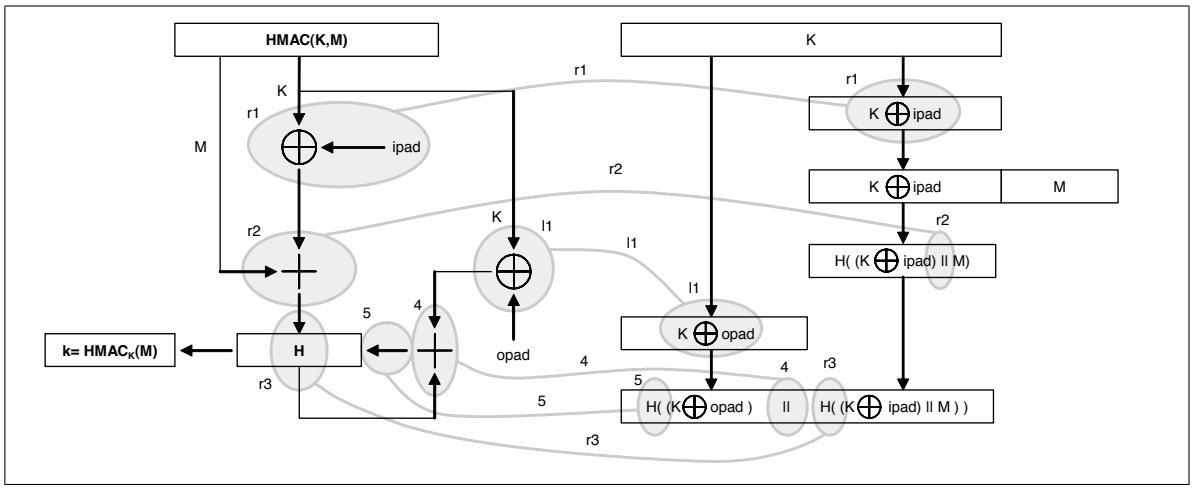

Figure 3.2: The HMAC Construction [6]

Two further strings with a fixed length of 64 bytes called "ipad" and "opad" which stand for the "i"nner and "o"uter bytes 0x36 and 0x5C are repeated 64 times respectively [152], symbol $\oplus$ denotes the bitwise XOR and a comma the concatenation of two bit strings.

Figure 3.2 illustrates the composition of the HMAC. The left side in this figure shows the plugging diagram of HMAC whereas the right side shows the corresponding iterative sequence. The HMAC computation starts with an alignment of the key K to meet the required length of 64 bytes. In the right branch of the sequence, the key is then XOR-ed with the 64 byte ipad (see step r1). The result of this operation is appended by the message M (see step r2) which is in turn applied to the hash function H in step r3. In the left branch, the key K is further XOR-ed in step l1 with the 64 byte opad. Now, in step 4 the intermediary result of the left branch is appended by the result of the previous operations of the right branch which results in a 128 bit string. This is applied to the hash function H which results in the final HMAC string.

3.1.5 Security Analysis of HMAC

Indeed, as already mentioned before, the introduction of HMAC was an important step to provide message authentication. Anyhow, it does not guarantee non-repudiation since the receiver of a message could have made the received data herself [152] (p. 10). Given this, the important question arises is how secure the proposed pseudonym generation scheme actually is? To answer this question best possible we continue with an explanation about some general assumptions that are essential to understand the basic principles of the pseudonym generation mechanism. After that, we continue with some fundamental security building blocks of the HMAC.

The security of HMAC mainly relies on the respective chosen underlying hash function. The HMAC construction allows different hash functions to be applied. The most prominent examples are MD4, MD5, SHA-1 or SHA-2. Whereas in section 3.1.1 p. 74 the general security requirements of cryptographic hash functions are explained, the following example,

illustrated by Bruce Schneier [150], aims to attain a better understanding of the whole matter. He states that for a given 64-bit hash value a computer that requires one second to compute the hash values of one million inputs requires 600.000 years to find the corresponding second hash value. But, in case a pair of inputs is provided to the same hash function with the result of the same hash value, the same machine requires only about an hour. The reason for this quite astonishing result is the so called *Birthday Paradox* which comes from probability theory. It explains why it takes at least time to find a pair of inputs that result in the same hash value and at the same time provides the answer to the question which of the three general requirements *Pre-image Resistance*, *Second-image Resistance* and *Collision Resistance* (see section 3.1.1 p. 74) is the most stringent one. Simultaneously, the answer to this question allows to determine the security of hash functions.

The *Birthday Paradox* states that there is a 50% chance to find one person out of 253 random people that has birthday on the same day as oneself. This question can be referred to the *Second-image Resistance* requirement. The second question that is referred to as *Collision Resistance* asks for the number of people required so that the probability that two of them have the same birthday is higher than 50%. Surprisingly, in this case only 23 people are required. The reason is that with 23 people it is possible to arrange 253 pairs. Seen from this point of view, the higher probability that one particular pair out of the 253 pairs yields a result is not only much easier cognizable but also probable from a statistical point of view. As a result, it is obvious that the most important requirement in terms of security of hash functions is the *Collision Resistance*. If a hash function cannot fulfill this requirement, also HMAC and hence the pseudonym generation scheme is not secure. There are however some more possible attacks such as *Collision Attacks on the key-less hash function*, the *Extension Attack* and the *Divide and Conquer Attacks* which are described by [152]. (p. 16) in *Keying Hash Functions for Message Authentication*.

The security of HMAC is very important for the proposed pseudonym generation scheme. Therefore, the following security analysis which is described in the position paper of ECRYPT (2005) [151] and also discussed by Bart Preneel and Paul C. van Oorschot in [156] is invaluable for the proposed scheme and can be seen as the basis of all the other security aspects that are related with the message exchange and the system architecture.

The security proof of HMAC depends mainly on the following two aspects. The first one is the choice of the respective underlying hash function HMAC operates on. Section 3.1.1 (p. 74) refers to hash functions that use a publicly known fixed initial value IV which is passed to the hash function's compression function. In contrast to the operation of hash functions, the security of HMAC depends on the security of the underlying hash function when the fixed initial value IV is replaced by a random secret value.

The second security aspect of HMAC asks for the predictability of the hash functions' output when, as the authors of [151, 153, 152] state, a secret text and/or a secret initial value IV is used. An attacker who finds a valid MAC without knowing the input may break the security of the underlying HMAC in either way by

- finding collisions of the underlying hash function when it is operated with a random and secret initial value or when
- an output of the compression function of the underlying hash function can be found when it is used with a random, secret and unknown initial value

Finding collisions of hash functions with a fixed initial value is very hard. But, it is even harder to find collisions if the initial value is secret because this kind of attacks requires the interaction with the user to be able to generate pairs of input/outputs from the function. Furthermore, HMAC does not allow parallelization of birthday attacks [153] (p. 3). Given the recent attacks it is rather doubtful to find collisions with random secret initial values. It is even more unlikely to find known outputs with this starting basis. If one finds collisions on standard hash functions this does not imply that it is possible to forge MACs. Thus, HMAC is secure unless more sophisticated attacks on hash functions are found.

3.2 Cryptographic Primitives and Security Services

Security services build the basis of all deliberations regarding the security and protection of services, systems and identities. All technical and also organizational means that are necessary to achieve secure services and operations can be break down into security services. A very good overview and explanation of the particular security services is provided by Pfitzmann [141]. In order to be able to realize such security services a number of cryptographic primitives are necessary. The combination of different cryptographic algorithms such as one-way-functions and encryption-decryption functions - also referred as cryptographic primitives - allow the development of complex protocols and security services. In the following we shortly discuss two such primitives *perfect forward secrecy* and *Malleable encryption*. Both are indeed only in certain cases important such as *Off-the-Record Messaging* which at the same time provides important aspects that are also effective for the proposed pseudonym generation scheme as well.

Perfect forward secrecy or simply *forward secrecy* stands for the indispensable protection of someone's privacy and refers to the inevitable protection of identifiers that, without proper safety measures, might reveal the true identity of a person. In this context in [157] I. A. Goldberg refers to the protection of the identity of the sender of a message "after the fact", that is, the protection after the message is sent. I. A. Goldberg provides as example an anonymity provider which should store no logs. Except from legal issues that may arise with the compelled storage of logs, we discuss later in section 4.6.3 (p. 124) that storage and confirmability of conversations may not only hinder social communication but that the abidance of forward secrecy is also a matter of the proposed pseudonym generation scheme which we discuss in detail in sections 4.2 (p. 97) and 4.4.3 (p. 116).

Malleable encryption which is described and used by Borisov et al. [15] for the realization of *Off-the-Record Messaging*. This requires that neither the intended receiver of a message nor any intercepter may be able to prove who the sender of the message actually is. Furthermore, malleable encryption requires that messages can even be altered by anyone. At first glance the latter requirement seems to be unfeasible for the realization of messaging systems that aim to provide secure communication. Borisov et al. further argues that *authentication* of messages based on encryption schemes that do not allow to receive meaningful plaintext without knowledge of the encryption key should be avoided and are rather evidence of poor practice. The use of stream ciphers instead of block

ciphers provides that any changes to bits in the cipher text affect only the corresponding bits in the plaintext. Even though in this mode neither the integrity nor authenticity of messages can be guaranteed, the sender may still use a MAC to prove authenticity.

We continue with a short discussion about some of the most important underlying security services.

Anonymity is achieved if a transaction reveals no information about the corresponding identity. This includes not only a particular transaction but also previous transactions. I. A. Goldberg [157] provides as an example purchases at the grocery store. If the client pays with cash, it is possible to avoid that any identity-related information is revealed. In case when total anonymity can be guaranteed I. A. Goldberg also refers to the notion of *unlinkable anonymity*. In contrast to that *linkable anonymity* concerns any transaction that does not reveal the respective identity but in this case it is possible to link transactions of a certain identity.

Linkable Anonymity refers to the case where the identity that initiates a transaction cannot be identified, but, the different transactions can be recognized and linked together. I. A. Goldberg [157] provides two examples for linkable anonymity. One is the prepaid phone card, as second example the frequent-purchase card is mentioned (p. 47).

Pseudonymity A pseudonym distinguishes from the *verinym* which represents the true identity that is for example the identifying information like the credit card or telephone number, street address, email address and in some cases even the ip addresss [157] (p. 41) to name only a few.t Pseudonymity is often conflated with anonymity. As I. A. Goldberg [157] states, these two security services represent the two forms of privacy of identity. They are are often summarized as *anonymity*. The use several pseudonyms for different transactions provides that it is not possible to reveal the underlying identity. Each pseudonym used for different purposes prevents from linking transactions. However, as we will discuss in section the use of permanent pseudonyms may also be problematic in terms of recurrent requests issued by the same identity. In this case, when one and the same pseudonym is used in succession, the owner of a pseudonym may no longer be in charge of control who has access to her identity.

(Un)linkability: Linkability and unlinkability are already discussed in terms of anonymity and pseudonymity and represent an important question especially in the light of pseudonyms. As the core mechanism of this dissertation is based on a scheme that generates pseudonyms that are not linkable, the notion of linkability is of special importance.

Integrity: Another important security service is that of integrity which is closely related with the requirement of confidentiality. Mechanisms which provide message integrity guarantee that data cannot be modified during transit. This kind of integrity refers to trustworthiness of data whereas another kind of integrity refers to the origin of data which is closely related to *authentication*. M. Bishop distinguishes in [155] p. 5. two further kinds of integrity mechanisms. One aims to *prevent* integrity violations whereas the second one aims to *detect* integrity breaches. In case of preventing from integrity

violations the attacker has no authorization to access the data whereas the second case deals with the problem of preventing modifications of data undertaken by persons who are indeed authorized to access the data but violate the integrity in another way.

Authenticity: Messages that can be assigned to a particular identity are said to be authenticated. This holds for electronic communication as well as for messages that are exchanged from face-to-face. As these two kinds of communication are fundamentally equal (sender - receiver etc.), it is however totally different carried out. Whereas electronic communication enables to communicate even over long distances, face-to-face communication also involves unique human characteristics that are inherent to human being and language. It is almost impossible to reproduce the richness of the human language and expressiveness electronically. One way to provide message authenticity is by means of cryptography.

Confidentiality: Alike authenticity also confidentiality is an important security service required for the realization of secure communication and concealment of information. One means to provide confidentiality is *access control*. There are many different ways to achieve confidentiality. One is by utilizing cryptography. This requires that the encryption scheme is secure and that the key is protected from unauthorized access wherewith the problem of keeping information confidential is not completely solved but rather shifted to another problem that is how to prevent from unauthorized access to the key. Beside cryptographic means there are also other ways such as an *access control matrix* to prevent from unauthorized access. In section 7 p. 160 we reference to advanced technologies that allow the realization of access control that is based on decisions made under the assumption of changing circumstances.

Non-repudiation In contrast to *Repudiation* which is discussed in section 4.6.2 p. 124 this security service prevents from repudiation of binding agreements or statements.

At the beginning of this section we already mentioned that *authentication* is the fundamental question in this dissertation. The proposed pseudonym generation scheme is primarily based on MACs which, as the name suggests, authentications messages. Authentication is also the subject of the following section. We will highlight some fundamental questions regarding authentication.

3.3 Authentication

Almost any communication, including face-to-face communication relies on some sort of authentication. When people communicate face-to-face with each other, they can see their counterpart. In case someone receives a phone call from a known person, this person can verify the authenticity on the basis of the recognized voice. In this case, the example of voice calls is indeed a good example to show, that the authentication in communication systems works. Meanwhile, the general conduct is that if we call a person which we know we have confidence that we are really talking to this person. Our ability to recognize the voice, the use of certain phrases or simply consent about a certain topic allows us to verify the identity of the respective counterpart. However, what if the two communication parties do not know

each other or even cannot rely on the heard voice or at least the number of the caller on the display of the phone?

The vast developments in communication systems has a tremendous influence on the traditional telephone systems. The changeover from the traditionally closed telephone system to an open system that uses advanced communication protocols on top of the internet protocol induces a number of challenges such as the development of new interaction models and protocols. With regard to authentication, the use of new technologies and interaction models requires much more efforts and in some cases even a change of thinking. Especially in terms of requirements for authentication, emerging communication systems differ substantially from the traditional telephone system and entail the development and use of e.g. cryptographic technologies.

This section discusses the most important aspects with respect to *authentication*. This is, along with other aspects discussed further in other sections of this dissertation one of the essential parts in secure communication. In the following we start with some basics about authentication and ask what authentication actually means?

Basic Principles and Definitions of Authentication

Bishop [155] (p. 309) explains authentication by means of the following three terms: *identity*, *subject* and *external entity*. The relations between them can be described such that, subjects that are related to external entities also act on behalf of them. According to that, each action that is undertaken by a subject has in turn to be controlled by the respective identity.

On the basis of this, Bishop provides the following definition:

"*Authentication is the binding of an identity to a subject*". [155] (p. 309)

The relation between an identity and a subject that acts on behalf of an entity is also implicitly contained in the definition of authentication given by Pfleeger *et al.*:

"*Authentication is basically a means of providing or verifying a previously given identity*" [87] (p. 619).

In order to be able to confirm an identity, the authentication process has to be provided with some information about the respective entity. Thus, authentication schemes are primarily based on the following qualities which describe what the entity, respectively the user

- *knows*: this includes all kinds of secrets and keys no matter if they are actually stored on the user's device or in one's head. Information that is stored on some physical devices leads to the next quality that is what the user
- *has*: this quality concerns things that are related to and applied in the physical world such as identity badges, physical keys or the driving license to name only a few. But, by way of example, technologies such as RFID relax the strict distinction of physical devices to pure members of the user's "*has*" properties. Thus, also physical devices can be subsumed as part of the previously mentioned quality "*knows*".

- *is*: which is probably most difficult to assess and in some cases even questionable. It describes unique physical characteristics of users and includes fingerprints, the retinal characteristics or the shape of the face.

- *where is*: this quality relates to the use of location as means for authentication. In this respect Bishop [155] (p. 331). describes a location signature that is generated by the user and that is sent to a host for authentication. Since this signature is generated with the available time and location information it is considered to be unique. A dedicated host authenticates the received signature. This scheme is intended to be used to grant access based on certain location signatures but can also be used conversely to prevent access.

After this discussion which should at first provide a general understanding of what authentication actually means, we now try to show a different definition of authentication with respect to different viewpoints. For that purpose, we deliberately omit a descriptions of the various existing authentication protocols and schemes and continue with a discussion that shows how authentication is separated from *identification* and the security service *confidentiality*. After that, we continue with a rather theoretical information theory point of view and conclude this section about authentication with an exception, that is, one of the most important to mention authentication schemes that are primarily based on hash chains. The reason why we anyhow discuss theses two schemes is because they are directly leading to our proposed solution.

3.3.1 Authentication and its Separation from Identification

After the preliminary considerations about authentication, we continue to look at how authentication separates from identification. Therefore, we first explain what an identity is and what constitutes an identity which allows us to define what the notion of *identification* exactly means. Starting from human beings as motivation for privacy, Pfitzmann *et al.* [141] (p. 28) defines an *identity* as

"*...any subset of attributes of an individual person which sufficiently identifies this individual person within any set of persons. So usually there is no such thing as "the identity", but several of them.*".

Pfitzmann continues that these certain subsets of arguments that constitute the identities of individual persons are certainly also subject to possible changes. In this context Pfleeger *et al.* [87] (p. 619) mentions authenticators which, in case of biometrics can be used for means of authentication. One or more authenticators like the fingerprint, the unique retina pattern or simply the whole face should result in exactly one identity or none. Based on authenticators, Pfleeger raises the question whether a given identity corresponds to the provided authenticators. This differs fundamentally from identifying an identity only by some given authentication data. One can ask, at which percentage does the process of authentication result in a match for that particular identity? The identification process is about to be successful if a certain threshold is being reached. However, there still remains open the question which percentage rate to chose as threshold to avoide wrong decisions. Conversely if only some authentication data is provided but the corresponding identity is known in advance, identification is much harder to achieve and needs some further investigation. The

reason why identification is much harder is that if only some authentication data is available, it is not sure if the corresponding identity can be found at all. Whereas in the first case the result of the authentication process may be based on some matching result which allows to derive some percentage value, in this case it may happen that given some authentication data none or even several identities are found. This circumstance makes it much more difficult to formulate a definite answer. As we will see later, the proposed pseudonym generation scheme avoids such ambiguities.

3.3.2 Authentication and its Separation from Confidentiality

It is not too long ago when *authentication* and *security* were not easy to distinguish. Eventually, cryptographers discovered that these two even have different goals and it turned out that authentication and security are, at least from a theoretical point of view, even incompatible [149] (p. 278). What looks a bit quaint at a first glance turns out to be an important building block for the analysis of these services.

In the following we reflect the explanations of Bavaud [149] who keenly discusses the distinction and incompatibility of *authentication* and *confidentiality* or rather *secrecy* from an information theoretical point of view (Bavaud [149]) (p. 62). But first, we discuss two basic concepts *mutual information* and *entropy* which are required in order to be able to understand the following discussion.

Mutual Information

We start with an important notion used in information theory, that is the so called *mutual information* between two random variables X and Y, that is

$$I(X|Y) \geq 0. \tag{3.2}$$

which describes the *expected measure of information* gained by observing whether some event takes place or not. In other words, it expresses the *expected amount of information* relative to X gained by observing Y. Without going into closer detail which means that we omit the line of argumentation, it is further stated that $I(X|Y) \geq 0$, and $I(X|Y) = 0$ if, and only if, X and Y are independent. Furthermore, there is also a symmetry in X and Y which can be expressed by $I(X|Y) = I(Y|X)$. This is because we can expect as much information on X by observing Y than on Y by observing X.

One requirement to ensure message *authenticity*, that is, messages are sent by an authorized person, is that the mutual information between cryptograms (C) and keys (K) must be big, thus $I(C|K) \gg 0$ ensures authenticity. To ensure message *confidentiality*, that is, messages are received by authorized persons, requires $I(C|M)$ to be as small as possible. *Perfect Secrecy* is achieved when $I(C|M) = 0$ (see Bavaud et al. [149] (p. 285)).

Entropy

Another way do describe perfect secrecy is by measuring the *entropy* that is basically a measure of the amount of uncertainty in a variable. Cryptographers and information theorists used it to determine how well transformations on messages obscure their meaning [155] (p. 935). In this sense, perfect secrecy can be reached if a random variable M that takes the values of a set of messages $m_1, ...m_n$ is used for the generation of the cypher $C = e(M, K)$ such that $H(M|C) = H(M)$ which means that knowing the cipher C does not decrease the uncertainty of the message M and equals the uncertainty of the message [155] (p. 940).

The One-Time Pad [149] (p. 259) is an example that shows how perfect secrecy can be met. An intercepted cipher gives no more information to the attacker since the key is randomly chosen and has the same length as the message. Thus, the uncertainty of the message is $H(M|C)$ and since any message could have generated the cipher. This means that $H(M|C) = H(M)$ and thus perfect secrecy is achieved [155] (p. 940).

We use the entity, in particular conditional entity in the following section do explain why authentication and confidentiality are incompatible, at least from a strict information content point of view.

Authentication vs. Confidentiality

Given message M and key K the cryptogram C is generated with a deterministic function such that $C = e(M, K)$. Thus, given M and K the entropy is $H(C|M, K) = 0$. Given a cryptogram C and a decryption function d the message can be received through $M = d(e(M, K))$. For this case the entropy is $H(M|C, K) = 0$. It is important that both entropies do not imply entropy $H(K|M, C)$. This, since there could be used several keys that are possible for the pair (M, C). However, in practice it is a better idea to use only one key, so from now on we can assume that $H(K|M, C) = 0$.

In the following it is stated: *The probability P_I that a cryptogram is falsified (i.e. to find a cryptogram that is accepted although it has not been emitted by an authorized person) is bounded by*

$$P_I \geq 2^{-I(C|K)} \tag{3.3}$$

The proof for this theorem is omitted here but can be found in [149] (p. 278).

To guarantee authenticity the mutual information between cryptograms and keys must be big, thus $I(C|K) \gg 0$, whereas to ensure perfect confidentiality $I(C|M) = 0$ is required.

The following formula shows the connection between authentication and confidentiality which, however, shows that there is an apparent incompatibility between these two, at least from a strict information content point of view.

$$I(C|K) = I(C|M) + H(K) - H(M) - H(K|M, C) \tag{3.4}$$

Since $I(C|M) = 0$ and with the assumption that in practice it is better to use only one key, $H(K|M, C) = 0$, authentication $I(C|K) = H(K) - H(M)$ now implies that $P_I \geq 2^{H(M)-H(K)} > 0$. The more complex key are used, the better. Thus, $H(K) \gg H(M)$. However, this also raises the probability that a cryptogram is falsified, which is a contradiction. To overcome this theoretical contradiction and anyhow ensure the possibility of

authentication, cryptographic systems are commonly based on algorithmic complexity. The most common way to achieve authenticity is by the use digital signatures which additionally provide *non-repudiation* (see section 3.2 (p. 79)).

Next, we discuss message authentication codes (MACs) which can also be used for authentication purposes. However, in contrast to digital certificates MACs further allow to relax the stringent requirement of *non-repudiation*. The resulting requirement of *repudiability* which is important for the design and implementation of *off-the-record communication* systems as it is proposed by Borisov et al. [15] and further discussed in relation to pseudonyms in section 4.6 (p. 122) is not only a contradiction to the security services provided by digital signatures. From this point of view it is possible to build electronic communication systems that provide a high security level and which converges with real-world *face-to-face* communication.

3.4 Authentication Schemes

Referring to the discussion about *authentication* and formal explanations on the distinction between authentication and other security services, we continue with a demonstration of well known and important authentication schemes. We discuss those schemes that utilize the security properties of hash functions. One such scheme is Lamport's authentication scheme. It uses hash functions and their intrinsic properties as the underlying mechanism, continued by the Time Efficient Stream Loss-tolerant Authentication scheme.

3.4.1 Authentication Scheme by Lamport

The idea to use hash values for authentication is not new. Among other solutions that are discussed in the following, we start by singling out the particular idea introduced by Lamport [7]. Later, various other solutions have been proposed and developed, with varying degree of success. The authentication scheme proposed by Lamport can be deemed as precursor of password authentication schemes that are based on hash values. It is based on message authentication codes and aims at removing the following weaknesses to protect the user's secret password:

1. *gaining access* to e.g. the system's password file or
2. *intercepting communication* which includes e.g. eavesdropping or any other means to retrieve the password
3. *inadvertent password disclosure* through the use of simple passwords that are guessed easily.

Because the last point may require additional and even complex technology it is - as in the original paper of Lamport - not considered a detailed discussion here. (remark: maybe it is possible to mention this in another chapter, give some example you can reference to?) Thus, only the first two problems of how to prevent from gaining access to the password file and intercepting communication are discussed.

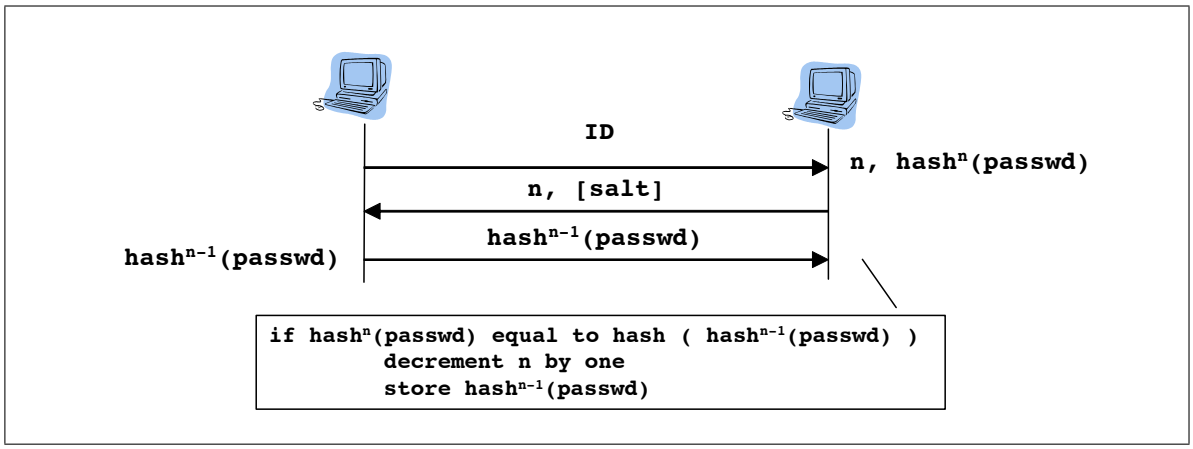

Figure 3.3: Lamports Authentication Scheme Based on Hash Values [7]

The solution to the first problem can be achieved by the use of a one-way function F. Therefore, the system stores not the password x itself but the encrypted version of the password, that is $F(x)$. According to the basic requirements of one way functions (see section 3.1.1 (p. 74)) it is guaranteed that given a value $y = F(x)$ it is indeed possible to find x, but requires vast effort so that attacks are effectively impractical. A system that stores only the value $y = F(x)$ instead of the password x in cleartext complies with the requirement stated in the fist point. Users may authenticate by sending the password x' whereupon the system computes $y' = F(x')$ which results in the same value y that is already stored by the system. If the $y = y'$ the user is authenticated.

However, referring to the above mentioned second point *intercepting communication* which does not protect the password during transit, Lamport mentions two additional schemes. The first scheme requires too much memory since it requires to store the entire sequence $y_1 = F(x_1), ..., y_n = F(x_n)$. The second scheme is insecure in terms of possible communication failure or interference caused by malicious users. After logging on with x_i during the i^{th} session the value y_{i+1} could maliciously be used by an intruder to prevent the system from learning the correct value of y_{i+1}.

Lamport argues that both solutions present only partly solutions which however can be combined in a way such that the best features of both of these schemes build up to the secure password authentication scheme which is now discuss in closer detail.

Lamport Authentication Scheme - Operational

The following explanations of the original authentication protocol is also depicted in Figure 3.3 and also presented by Schneider [158]. If the client wants to authenticate, it first sends a request for login to the server which responds with a challenge n. The salt is optional. The client may now calculates the n-1$^{\text{th}}$ hash value of the shared secret s and sends this value back to the server. Upon receipt, the server first hashes the received value $h(h^{n-1}(s))$ and compares it with the stored n^{th} hash value of the password $h^n(s)$. If the received value is equal the stored one, that is $h(h^{n-1}) = h^n(s)$, the authentication was successful. Then the server decrements n by one and replaces $h^n(s)$ by the next (prceding) hash value $h^{n-1}(s)$. For

the next authentication, the client receives the chalenge $n-1$ and responds to the server with $h^{n-2}(s)$ which compares the previously stored value $h(h^{n-1}(s))$ with the rehashed received value $h(h^{n-2}(s))$.

Large n attack on Lamport's Authentication Scheme

Although Lamport's Authentication scheme is very secure there is however an attack which is known as *Large n attack* and also describe by Schneider [158]. The attack assumes that from a single secret first a sequence of 1000 passwords is generated. As the number n becomes close to 1000 an attacker who knows a password, that is generated with such a high value, ultimately knows most of all the 1000 one-time passwords of this chain. If the second message is not secured in a way such that the client cannot prove the authenticity of the server, an intruder may impersonate the server and send n close to 1000 as challenge. Now, the intruder knows most of the one-time passwords of the user.

3.4.2 Time Efficient Stream Loss-tolerant Authentication (TESLA)

The implementation of the TESLA scheme is mainly based on Lamports authentication scheme. By adding asymmetry through delayed key disclosure and loose synchronization between sender and receiver the TESLA scheme further provides means to allow not only point-to-point communication but also broadcast/multicast communication. The TESLA scheme is described in detail by their authors in RFC 8042 [159]. The distinction between authentication and identification in point-to-point and broadcast/multicast communication environments is essential. In case of point-to-point communication, the receiver can easily verify the authenticity of a message and the identity of the originator of that message by means of message authentication codes. If the same scheme is applied in a broader scope, that is, in a broadcast/multicast environment, all receiver of a communication group also need to know the shared secret that is used to generate the MAC. The reason why this scheme cannot be applied in group communication such as broadcast or multicast is that even though every receiver of a message can verify the integrity of the message it is not possible to proof the authenticity of the sender. Authentication that uses asymmetric cryptography such as digital signatures indeed provide a solution to uniquely identify the sender. However, such solutions are not applicable in ad hoc networks or in any other application field that innately provides only limited computational resources. Equally, administration of pairwise keys that are shared between the respective communication parties is highly inefficient and does not solve the problem adequately [8]. In the broadcast and multicast domain the TESLA scheme uses symmetric cryptography for authentication and identification. Loose time synchronization and the delayed key disclosure allow for secure communication among the involved communication parties. The following brief description of the basic operations of TESLA refers to the description given in [8].

TESLA scheme - Operational

Before the sender can send data to multiple receivers, he generates a secret key that is denoted K. This key is needed to initialize a hash chain that is analogous to the key-chain introduced by Lamport [7] and which is discussed in closer detail in Section 3.4.1 (p. 86). The sender

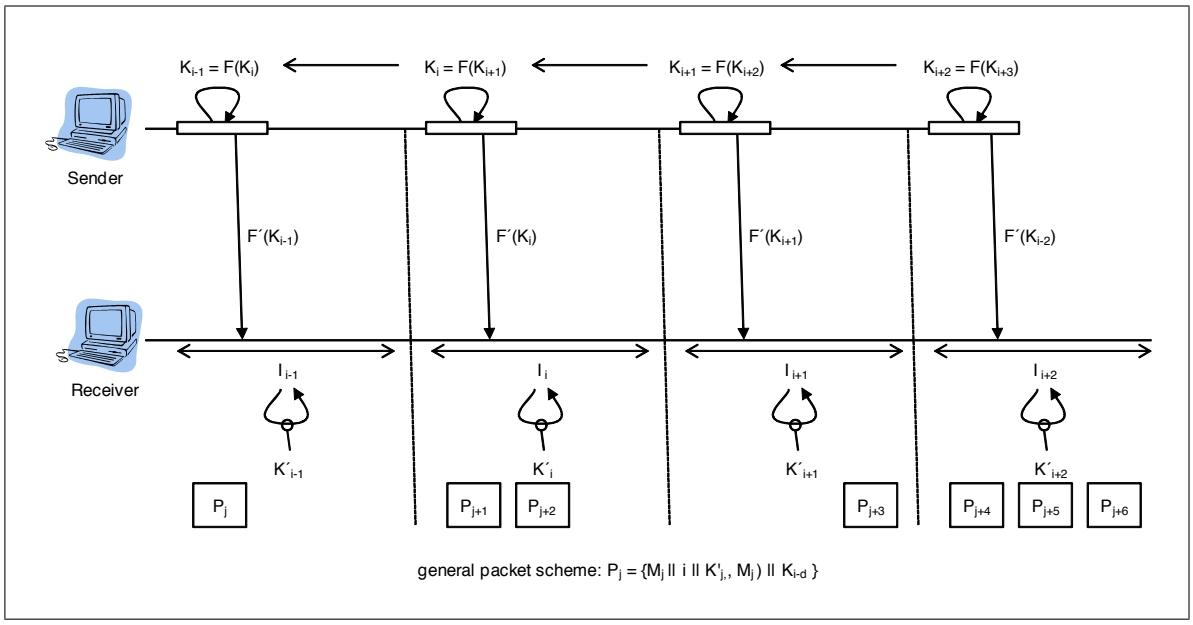

Figure 3.4: Timed Efficient Stream Loss-Tolerant Authentication (TESLA) [8]

then determines a number of time intervals which is correspondent to the number of elements of the hash chain that is next generated. Each single hash value of that chain is used for only a single time interval. In order to prove authenticity of the hash chain, the sender also generates a signature σ from the last hash value of the hash chain $h^n(k)$ which is also referred as K_0. The signature is generated by the sender with its private key. All receivers may verify the correctness of the signature with the corresponding public key of the sender. At this point we want to mention that in our explanations we do not consider the duration of a time interval T_{int} since it is not too important for a principal understanding of the functionality of the TESLA scheme. For a detailed discussion on that issues we refer to the papers of the authors of the TESLA scheme [8]. One important parameter the sender has to determine during the initialization phase is the key disclosure delay d and represents the numbers of time intervals a key is disclosed. Keys are disclosed in $i + d$ intervals whereas for $d > 0$ the TESLA scheme is assumed to be secure.

After the initialization phase the sender may now send out the broadcast messages to the receivers. The general packet scheme $P_j = \{M_j||i||MAC(K_i, M_j)||K_{i-d}\}$ is also shown in figure 3.4. Index i is the key index whereas j stands for the current interval. According to the general packet scheme each packet P_j contains the message M_j, the key index i and a keyed MAC. In each interval it is possible to send several packets. In each interval only one key can be used from the key chain. The key used for the generation of the MACs is not the key from the chain. This is to avoid that the same key is being used multiple times in different cryptographic operations. [160]. According to the scheme $K_i = F(K_i)$ (shown in figure 3.4) it is obvious to use HMAC as the underlying pseudo-random function. The elements of the key chain are defined as $K_i = F(K_{i+1})$ and can also be derived from $K_i = F^{N-i}(K_n)$ where N is the number of keys of the key chain and K_N denotes the last key of the chain.

In the following the receiver performs four steps of verification [159]:

1. The *safe packet test* first causes the receiver to calculate the upper bounds of the senders clock and then, based on that time, to calculate the highest possible interval x the sender could possibly be in. If $x < i + d$, that is the calculated highest possible interval is less than the interval that is provided in the packet plus the key disclosure delay, the packet is assumed to be valid. This means that the packet was not disclosed in during the interval when the sender disclosed the key K_i. Regardless of whether a packet can be verified or not, the receivers can decide to accept or drop the packet.

2. the *new key index test* checks that key K_v has not already been disclosed as current key K_{i-d} but with the same index v or a later one $v \geq i - d$.

3. the *key verification test* tests whether a disclosed key is valid or not. Therefore an earlier key $K_v(v < i - d)$ is verified by applying the hash function $K_v = h^{i-d-v}(K_{i-d})$. Packets that contain a key that could not be verified successfully should be discarded.

4. the *message verification test* checks the MAC of buffered packets. Therefore, the key K_{i-d} disclosed in the current interval is used as a basis for the calculation of the key that was used for the generation of MACs from packet in earlier intervals.

   Given any disclosed key and $i - d - v > 1$ it is possible to verify all available buffered packets that were received in earlier intervals.

   According to the general broadcast packet scheme and by assuming a key disclosure delay of $d = 2$ the packet P_{j+4} received in interval I_{i+2} discloses Key K_{i+2-d}, that is K_i. Given this key the receiver may even derive K_{i-1} and verify packet P_j.

The TESLA scheme represents an example how hash chains can be used for data packet authentication and integrity check in broadcast and multicast environments. Since the use of asymmetric cryptography such as digital certificates are computational expensive in sensor-networks and mobile devices the system uses symmetric cryptography only. Symmetric cryptography is about 3 to 5 orders of magnitude more efficient than asymmetric cryptography [159]. The required asymmetry is achieved through delayed key disclosure and loosely time-synchronization between the sender and the receiver. As indicated, the TESLA scheme is not restricted to point-to-point communication but can also be applied even in resource-constrained broadcast/multicast environments such as ad hoc networks.

Chapter 4

A Location Service Platform with Privacy Protection: Concept and Design

In the first part of this section we discuss the network operator's services and its basic functions. This is followed by a short review about the pseudonym generation system. This is extended by explanations about the service operations which include the initialization of pseudonyms, the subscription procedure and how users may then submit requests to receive enriched location information about herself or other users. We conclude the first part of the explanations on the location service platform with a short discussion concerning the communication capabilities of the system, the classification of the system and which kind of applications to be realized on top of the platform.

In the second part we go into further detail about the system interactions by discussing dedicated details of the underlying communication patterns and mechanisms that were in the first part of the discussion intentionally omitted. These patterns represent a basic block for the realization of a tracking platform which allows for the realization of location-based services and applications that process user's privacy sensitive data under compliance with stringent privacy protection guidelines.

4.1 System Architecture, Components and Basic Service Platform Interactions

Unlike the explanations given in section 2.3.3 (p. 42) which, from a business model point of view, clearly show how the proposed system architecture differs from traditional service architectures, in this section the focus is rather on the technical aspects of the system architecture. We also consider general security and trust requirements which are essential for the secure operation of such heterogenous systems provide a description of the basic operations as they are required for the operation of reactive LBS. This discussion also reports on the different security levels that are imposed by the heterogeneity of the used services that are in addition operated in different trust regions. For a better understanding, one description concentrates

rather on the different technologies and services that in sum are necessary for the realization of different kinds of location-based services. Another focus is the communications part that points out the needs and requirements that have to be achieved to trade off varying security levels, trust models and constraints imposed by equally varying conditions.

Figure 4.1 (p. 93) depicts the various services, components and software modules that in sum represent the technological basis for the realization of different kinds of LBS such as location-aware or location-tracking applications as described in section 2.2.7 (p. 27).

4.1.1 Some Preliminary Assumptions and Clarifications

The boxes on the left side shown in figure 4.1 (p. 93) represent two clients, namely the watcher and the presentity. It is assumed that the watcher requests the location of the presentity. With the location information received from the network operator the application service provider may generate added-value services to the users. This suggests, that clients are opposed to basically two different trust levels. One is represented by the sum of services that are offered by the network operator. As the user commits to provide the network operator with privacy sensitive information, the network operators enjoy a very high trust level. Contrariwise, this also bears a burden to the network operators who are confronted with legal changes and political pressure such as the European Data Retention Directive 2006/24/EC [97]. With the user's signature the network operator has to guarantee the confident handling of any personal data. This also concerns data that is generated by the network operator during operation and includes amongst others the user's location information. For further reading on privacy sensitive data generated and processed by the network operators we refer to section 2.4.5 (p. 58). The figure also shows two grey bars. One connects the users privacy agents with the network operators' privacy service. The second one connects the service provider's privacy agent with the privacy service. Both represent the trust relation between the privacy agents of the users and that of the service providers with the network operators privacy service that is implemented by the use of pseudonyms. With the aid of the pseudonym mechanism the user's privacy is protected in many respects. First, users retrieve information about other users only if they are entitled to. This requires the consent of the respective other user which is described as subscription process detail in section 4.4.3 (p. 116). Second, the use of pseudonyms veils both identities, that of the requesting user and that of the user whose location is asked for. This guarantees user anonymity towards the service provider which in turn creates user's trust towards applications offered by per se untrusted application providers. Furthermore, the pseudonym generation scheme represents a viable mechanism that can also be used for the authentication of application providers which makes other more complex and costly authentication schemes obsolete.

Client Device

Users interact with the system either via a high-end-PC, a cellular phone or a personal digital assistant (PDA) with wireless access. In case that the client device is connected to or, as an increasing number of new devices, have a built in a GPS receiver chip, the GPS software module that is part of the mobile application software receives the current location data which can then be used for the provision the location service. In section 5.7 (p. 143) the different

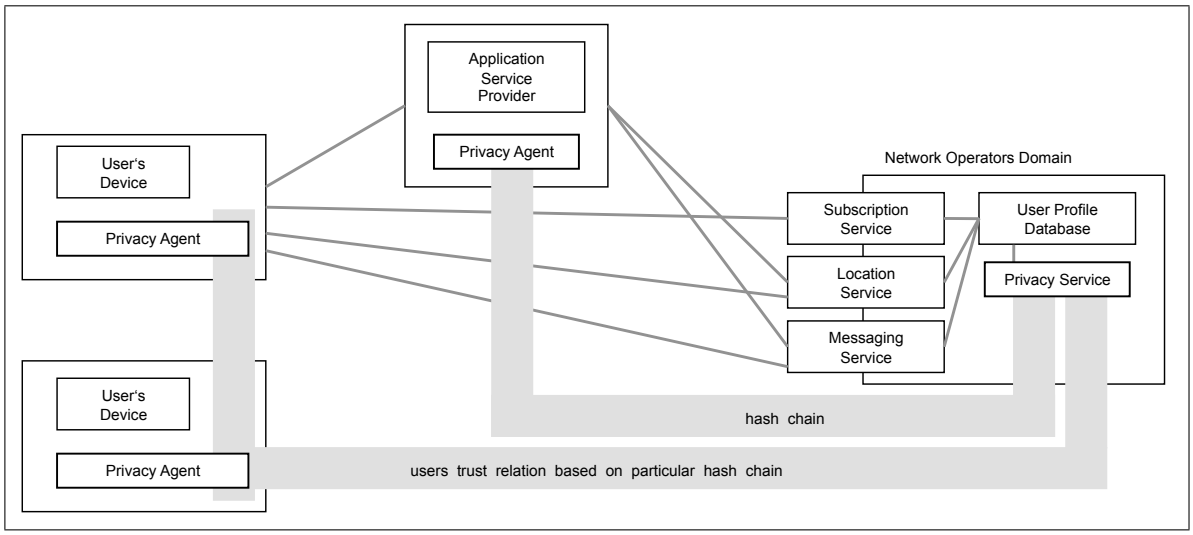

Figure 4.1: System Architecture

possible location update strategies are analyzed with regard to different considerable aspects such as network utilization, energy consumption and the question of the effectiveness of the strategies with respect to up-to-dateness of location data.

We clearly focus on cellular phones and PDAs with limited computation power, storage capabilities and restricted means of communication. But, this does not exclude devices which provide additional communication components such as e.g. Bluetooth. As many of these auxiliary technologies such as Bluetooth or GPS are meanwhile built in most mobile devices, we do not neglect these technologies but at this point rather refer to a latter section (see section 4.4 (p. 111)) because focus here is on the network based localization that is exclusively provided by the network operator's only and does not require additional communication capabilities from mobile devices. If if GPS data is available, the application logic shall provide means that enable users to choose from different available update strategies. Furthermore, this includes the possibility to stop location updates et all. This applies to any kind of client and in general any localization technology and thus represents a common requirement that stems from the user's self-determination. The application's logic is further responsible for the control and visualization of user's interactions and the flow control of the software as a whole.

Each client as well as the 3^{rd} party applications and the network operator's privacy service implement a dedicated module that is the so called *privacy agent*. This module is responsible for the generation and management of digital pseudonyms as they are discussed in detail in section 4.2 (p. 97). Pseudonyms are generated on the basis of attributes which are stored by the network operator's user profile database. Beside creation of pseudonyms it is also responsible for the management thereof.

3^{rd} Party Application Provider

Depending on the users choice which application to use, the requests and pseudonyms are routed through one or more 3^{rd} party application provider. For that it has to provide the

appropriate interfaces towards both, the users and to one or more network operators. The link between the application and the network operator may be secured to prevent various possible attacks by means of SSL. A prerequisite is mutual authentication. Since applications may communicate with several different services (location, messaging, presence service) of the network operator, for each communication line dedicated digital certificates are issued.

Whereas the security efforts needed to protect the communication links between the application and the network operators services are high, the other side the communication link, that connects the users and the application is solely secured by the use of digital pseudonyms and additional hash values that are used as fingerprints and guarantee data integrity. This simplicity allows to keep the interfaces as simple and generic as possible. Furthermore, the less processing is needed, the faster the communication can take place. Without the need to mutually establish connections users may send requests even asynchronously.

Some services that are provided by applications may operate on totally anonymous data. In some cases it may make sense to provide static pseudonyms such as alias names. One example where some kind of identification makes sense is an application that displays the positions of several users or objects on a map at the same time. Even though neither the real name nor any other privacy sensitive data is revealed, labeling each shown position with the user's nickname may affect the user's privacy. It is therefore important to provide means that allow the users to decide and be in charge of if and which data is revealed to 3^{rd} party application providers. As 3^{rd} party application providers are per se not trusted it is the network operators responsibility to provide appropriate means.

Network Operators' Services

Mobile Network Operators maintain the whole infrastructure that is necessary to provide speech, messaging and data services. With the introduction of the Universal Mobile Telecommunications System (UMTS) which is also known as third generation (3G) network most mobile network provider complemented their network to allow higher data transfer rates and services. Different kinds of services include speech, messaging and mobile television. Together with faster internet access, location and presence services mark a turning point for operators to provide services also to service providers.

Standardization initiatives such as OSA/Parlay X [85] that aim to provide uniform interfaces foster the development of applications provided by service providers that make use of the network operators infrastructure.

Location Service The location service we consider in this discussion is located within the network operators domain. Like any other location services it provides different interfaces that allow users to request and update location information. Furthermore, the location service has access to or is part of the mobile network infrastructure and may query the actual location of mobile terminals. Therefore it queries the location server that is also part of the network and has accesses to the user's location data.

It is also conceivable to operate the location service outside the trusted domain of the network provider. In this case the stored location information has to be protected against unauthorized access. In this case it is necessary to provide means the allow to store and process only anonymized location data. The discussion in section 4.5 (p. 121) shows a

generic database scheme that can be applied for the operation of the location service that is located in the trusted domain of the network operator. In case the location service is operated outside the trusted domain, the database scheme has to be adapted to meet the required user anonymity.

Privacy Service The privacy service represents the server-side implementation of the user's and application's *privacy agents* that are implemented on the client device and the service provider respectively. Basically its purpose is also quite similar, that is, storage, management and processing of pseudonyms. Different to the privacy agents that generate and send pseudonyms, the privacy service receives them on request and generates the respective next pseudonym for subsequent requests. Each pseudonym represents a user-relationship. Depending on the user's role the privacy service administers basically two kinds of pseudonyms, that are, self-identifying pseudonyms. The second kind is used to represent the relationship between two different users. One takes the role of the so called *watcher*, the respective other one whose location is asked for is the *presentity*.

There is even a third kind of pseudonyms that can also be related to self-identifying pseudonyms. This is the pseudonym used by the service provider. Just as the self-identifying pseudonyms it allows service providers to authenticate. Technically all these pseudonyms are equal. The only way pseudonyms are distinguished is by who generates the pseudonym (who is the owner) and who else is referred (the owner or presentity).

Authentication of users subsequent identification of user relations is one thing. By knowing who requests information about whom the privacy service may now further take into consideration the type of request and which application the user called. Furthermore, the privacy service may administer or have access to all user profiles which can be subsequently used to decide whether access to the location information is granted or not. Another important input is which request the user submitted (e.g. `getLocation`) to which kind of application? The latter question can be answered by the privacy service with the help of the provided application pseudonym. Just as the user profiles, the privacy service may also access application profiles. These profiles encode amongst other information descriptions of the interfaces in e.g. WSDL (Web Service Definition Language)[161]) format. It explains how the application can be contacted, what additional information is necessary and which formats. With this information the location service knows the address and other important contact details of the service providers and the required format of the location information.

One possible way how all this information about the user(s) and application profile(s) can be processed and aggregated under consideration of the different existing obligations, be it legally, user defined or simply caused by technical means is by introducing a context server. This not depicted in figure 4.1 but further discussed in [162] by Zeiss and Jorns.

A certain type of location-based services such as tracking services require that localizations can also be performed over longer periods of time but without the necessity of additional user intervention. This requires session management. The privacy service and the location service are the only services that may process those user's identifiers that may reveal the identity of individuals. In case the location service is part of the network operator's domain, it stores the location data in association with one or more

user's identifiers. One such possible identifier may be the MSISDN, but this depends on the respective implementation at hand. However, if the location service is positioned outside the trusted domain of the network operator, some additional measures such as anonymous identifiers that are assigned temporally by the privacy service to protect the identity of users are required. Similar to that, service providers should per default operate on anonymous data. But, there are also certain applications, where total anonymity does not pay. Consider for example a simple tracking service that simultaneously displays the location of several user's buddies on a map, possibly including the requester's own position. If this application operates on anonymous data only, the more people the application tracks, the more difficult it becomes for the receiver to distinguish each tracked user. In this case total anonymity towards the application makes no sense. The solution to this is to allow users to publish their alias names to the service providers where this makes sense. This indeed amounts to an intentional privacy degradation which in our opinion can be accepted.

For proactive, single- or multi-target applications (for a detailed discussion regarding possible classifications we refer to section 2.2.6 (p. 24) which rely on long-term localizations and processing capabilities a session identifier is needed. Each session can be referred to this session identifier which ties together several localization processes to one logical process.

Especially for proactive location-based applications that highly depend on up-to-date location information of users the implemented interaction patterns should allow to detect and as needed instantly convey user's location changes. The certainly also effects questions regarding the scalability of the system which is however out of scope of this dissertation.

Messaging Service The presence status of users can be expressed by a vast number of attributes and can even be derived from the location information. Examples of the most important *activities* may include "going by car, waking, waiting to name only a few. Also *communication means* including the e.g. bandwith *contact addresses* (email, SIP, mobile,...), *location type*, *mood* (happy,...) and *privacy* (can talk). Of course, this list is by far not complete but it gives an idea of the potential sensitivity of that information. All these states may also be reflected by a presence service that aggregates different information sources and determines the respective state. However, the list of possible states is tremendous and does not significantly increase the expressiveness, we believe that for most purposes simple descriptions and characterizations of situations are sufficient enough. A reduced set of presence states further allows for client side implementations.

An essential part of the system is the ability to inform users asynchronously about certain applications' states which depend on the location information received from the location service as well as the current presence status of user. In order to receive the appropriate destination address(es) the messages service and the presence service work closely with each other. Given the session context and the pseudonym based privacy enhancing mechanism the user's privacy remains preserved.

Subscription Service The subscription service provides a web-based interface to allow users to access the privacy service for management and administration purposes of pseudonyms, aliases and privacy access rules. In this respect, the subscription service's responsibility is to provide means of (re)initialisation of pseudonyms between two entities (user - user, user - object) in case that pseudonyms are out of sync and coordination during the subscription and authorisation phase between the watcher and the presentity. Section 4.3.1 (p. 101) provides the technical details about the subscription process.

The discussion so far focused on the particular services of a system architecture as it is depicted in figure 4.1 (p. 93). Except for the case of the location service which, as explained, may be either part of the trusted network operators domain or be located outside the trusted domain and be operated by a per se untrusted service provider, we did not discuss other possible architectural designs here. For that we refer to section 2.3.3 (p. 42) which provides explanations on the architectural decisions from a business point of view, why the proposed architecture was chosen and what benefits can be expected.

In the following we continue with a description of the pseudonym generation scheme which is mainly managed and operated by use of the user's and application's privacy agents and the server side implementation that is the network operator's privacy service. Without going into too much detail, we also highlighted the different security and trust levels that have to be considered especially when designing distributed systems in heterogenous environments. This can be used for further studies and as such the derivation of an analytic model such as a detailed security analysis via e.g. BAN logic[1].

4.2 Proposed HMAC Pseudonym generation Scheme

Whereas in the previous section the focus is on the system architecture, its requirements and functionalities of dedicated services and components the system architecture is built up, this section explains the use of the pseudonym generation scheme and out of it the interworking of the services. This is of particular importance since it allows for the secure communication of users and thus represents a kind of connecting link between the requester, the service providers applications and the network operators services.

In a nutshell, each pseudonym is a so called *keyed-Hash Message Authentication Code*, short HMAC. The cryptographic details regarding HMAC are discussed in detail in section 3.1.3 (p. 76) by Bellare et al. [152]. According to a predefined scheme, for each service request, a user first has to calculate a pseudonym. The calculation of the first pseudonym relies on the previous initialization of the so called *self-identifying* pseudonym which is described in detail in section 4.4.2 (p. 113). This self-identifying pseudonym is used together with an initial value to initialize the pseudonym chain. In section 4.4.3 (p. 116) we discuss in detail how pseudonym chains are initialized and how they are used subsequently for the first service call.

We suppose that each user who has a contractual relationship with a network provider choses a personal master password during the registration process. This master password is then further used as the basis for the generation of individual secrets, each used for the

[1]The BAN Logic of Authentication: http://www.csci.csusb.edu/dick/samples/BAN.html (last viewed: 28. Mar. 2009) refers to Burrows et. al. [163]

generation of dedicated pseudonym chains. Since only a single user chosen password may not provide enough security for the generation of different pseudonym chains, the setup of each pseudonym chain further induces the generation of a dedicated shared secret. Each such generated shared secret is derived from the personal master password. For the sake of simplicity we also omit a detailed description of how these dedicated shared secrets for each pseudonym chain are generated. Instead, in this section we rather concentrate on the pseudonym generation scheme itself. The registration process is described in detail in section 4.3.1 (p. 101).

The pseudonym scheme proposed by Jorns et al. [164, 165] uses the HMAC, a keyed hash function by Bellare et al. [152] as the underlying cryptographic function (see also section 3.1.3 (p. 76)) for detailed explanations of the HMAC construction). The first parameter is an input value whereas the second parameter is destined for a shared secret. Each single pseudonym is part of a dedicated hash chain which is the result of recurrent HMAC function calls. Each pseudonym is the result of a HMAC function call which, except for the generation of the very first pseudonym, requests as input the respective previous pseudonym together with the shared secret for that particular chain. The very first pseudonym constitutes an exception in the sense that at this stage no previous pseudonym exists which can be used as input. Thus, the initialization of a pseudonym chain does not only include the generation of a dedicated shared secret for this chain but also includes the convey of a random number or string to the user that is used as the initial input value.

The following equation explains the general pseudonym calculation scheme:

$$h_k^i(r) = h_k(h_k^{i-1}(r)), \quad i = 1, 2... \tag{4.1}$$

It denotes the keyed cryptographic function (HMAC) as h_k with input r. The value of r basically depends on two things. First, it is decisive which kind of pseudonyms is to be generated. That means, whether it's a question of a self-identifying pseudonym that refers to one and the same identity or a pseudonym that denotes a particular person different from the owner of the pseudonym. In case of self-identifying pseudonyms the initial input value for the verify first one is the result of a Diffie-Hellman key exchange. For a detailed discussion on initializing self-identifying pseudonyms we refer to section 4.4.2 (p. 113).

The calculation of pseudonyms that refer to other persons than the owner use the alias name of that respective user. In the same way, for each pseudonym chain different shared secrets k are used. Regarding the shared secrets of pseudonyms, in a latter chapter we will discuss the issue of the necessity to change shared secrets and other factors that are decisive for frequent shared secret.

Finally, the index variable i denotes the number of the current function call. The equation above further shows that the i^{th} pseudonym is calculated on the basis of the respective previous $i - 1^{th}$ pseudonym.

After this short review of the pseudonym generation scheme we continue with another important issue that is already mentioned in the introduction, that is performance. As the security aspects of the pseudonyms are indeed closely related to performance questions. In section 3.1.5 (p. 77) we discuss the security aspects in detail and provide an explanation of the underlying cryptographic basics regarding the HMAC construction.

It is clear that there exist a variety of possible constrains and bottlenecks, each of them have a more or less impact on available battery resources, computing power and network bandwidth to name only a few. All these aspects have to be considered carefully especially when dealing with mobile devices. There is certainly a huge number of possible other factors that may be of importance. One such example is the right choice of the location update strategy of mobile devices. This issue is discussed in section 5.7.1 (p. 143) and is certainly representative as it touches many of the so far mentioned limits of mobile devices as well as cost factors. In the following we discuss the question how costly the calculation of pseudonyms actually is. Additionally, we show the efficiency of the proposed scheme compared with other schemes.

4.2.1 Performance Calculations

This subsection analysis the performance of the proposed transaction pseudonyms calculated on mobile devices. We also compare the obtained results with another authentication scheme, in particular with that proposed by Lamport (see section 3.4.1 (p. 86)) and show why the current mobile device's software technology is not suitable for the operation of this scheme.

Before we concentrate on the particular measurements we start with a brief overview of the environment. We deployed a J2ME WTK (Wireless Toolkit for CLCD(Connected Limited Device Configuration)) 2.5.2 [166] emulator [167]. Independent of the respective underlying platform, this toolkit basically provides built tools an emulator and allows integration of various APIs which are defined through the JCP (Java Community Process)[2] which includes amongst several others the *Mobile Service Architecture* (JSR 248), *Security and Trust Services API for J2ME* (JSR 177) and *Location API for J2ME* (JSR 179)t. A comprehensive list which includes all APIs that can be integrated is published by SUN[3].

A feature of the emulator that is important in the context of performance measurement is that it allows to adjust certain operating speeds of the mobile device. A dedicated list of currently available MIDP Java phones with various different performance values is published on the website of [168]. The emulator allows us to adjust the emulated speed of the mobile device within a range of 100 bytecodes/millisecond to 1000 bytecodes/millisecond. At the very beginning we observed, that without emulating the speed some calculations are too fast to be recognized properly by the system. More precisely, the system times measured before and after the calculation of a hash value is often equal. Surprisingly, we obtained the same results from tests on real mobile phones. Only when the emulator is adjusted to 100 bytecodes/millisecond, we received meaningful measurements. Through this justification the required time for the calculations can be translated for any mobile device by looking up the specification.

In order to back up our results we also conducted measurements on the OpenMoko mobile tri-band GSM device [4] with a ARM920T processor operated at a clock speed of 400MHz.

Apart from general programming practices that should generally be considered, software

[2]The Java Community Process (JCP) Program Management, URL: http://jcp.org/en/home/index (last viewed 6. Jul. 2009)

[3]Sun Java Wireless Toolkit 2.5.2_01 for CLDC Download, URL: http://java.sun.com/products/sjwtoolkit/download.html (last visited 6. Jul. 2009)

[4]OpenMoko URL: http://www.openmoko.com/ (last viewed 10. Nov. 2008)

Function	mean (ms)	var	median
HMac-MD5	245.75	313.8257576	250
HMac-SHA-1	462.64	503.5256566	453
HMac-SHA-224	806.40	610.5858586	797
HMac-SHA-256	808.12	488.8339394	797
HMac-SHA-384	928.91	658.9918182	938
HMac-SHA-512	1079.2	846.3838384	1093

Table 4.1: Measurements for the Calculation of HMac Values on J2ME Emulator

Function	mean (ms)
HMac-MD5	1.315029
HMac-SHA-1	1.64711
HMac-SHA256	1.438296
HMac-SHA384	1.82654
HMac-SHA512	1.844383

Table 4.2: Measurements for the Calculation of HMac Values on OpenMoko Mobile

that is developed for mobile applications and aimed to run on devices with only limited speed, memory and battery capabilities need special and critical performance considerations [169].

4.2.2 HMAC measurements

We start with the HMAC measurements shown in table 4.1. The first column stands for the respective function, the remaining columns contain the mean value, variance and median. The results are obtained from 100 calculations for each function on the J2ME emulator. At first glance the difference between HMac-MD5 and HMac-SHA-1 (first two lines of the table) is significantly high. HMac-SHA-1 requires almost twice as much computation time as HMac-MD5. This is clearly legible for both, the mean value and the median alike. Also the calculation time for HMac-SHA-224 is much higher than it is for HMac-SHA-1. The relatively minor increased length of bits (from 224 to 256) explains the quite similar results obtained for HMac-SHA-224 and HMac-SHA-256. The next significant difference is achieved for HMac-SHA-512. Now the median reaches a value above one second. By way of comparison, the second table 4.2 shows the measured times received from the OpenMoko device.

4.2.3 Hash value calculations

The next table 4.3 shows the measured times for the calculation of single hash values. By comparing MD5 with HMac-MD5 it shows a huge difference that at a first glance might imply that the use of HMAC is ineffective. But, MD5 and all the other shown functions in this table cannot be applied to the pseudonym generation scheme in the same sense as we can do with HMAC. Authentication schemes that are based on unkeyed hash functions discussed in section 3.1 (p. 73) which mainly rely on the intrinsic property called *Collision Resistance* which we

Function	mean (ms)	var	median
MD5	49.18	76.93549383	47
SHA-1	94.99	265.7877778	94
SHA-224	139.2	506.0400000	140
SHA-256	139.21	474.7736364	141
SHA-384	183.44	604.1680808	203
SHA-512	187.32	531.9773737	203

Table 4.3: Calculation of 100 Hash Values

Function	total time	mean (ms)	var	median
MD5	252527ms (4.20878333min)	50.00534653	49.07364936	47
SHA-1	478942ms (7.98236667min)	94.84	302.6711666	94
SHA-224	705941ms (11.7656833min)	139.790297	480.9421518	141
SHA-256	711889ms (11.8648167min)	140.9681188	485.712392	156
SHA-384	918814ms (15.3135667min)	181.9433663	628.2911077	203
SHA-512	944049ms (15.73415min)	186.940396	532.0913169	203

Table 4.4: Calculaton of 5050 Hash Values

discuss in section 3.1.1 (p. 74). This kind of authentication scheme and the results received from the performance measurements is shown in table 4.3. The calculation of a SHA-512 hash value requires even less time than HMac-MD5. But, if it is applied to the authentication scheme proposed by Lamport, then the results received differ significantly (see table 4.4).

4.3 Service Operations

After an explanation of the most important components of the system architecture and performance aspects of the pseudonym generation scheme, we now continue with a description of the operational part of the location-based service platform. In section 2.2.6 (p. 24) we already discussed the different kinds of location-based services. The following explanations refer to the group of so called reactive location-based services. This kind allows only synchronous message interactions and requires users to actively submit location requests.

Prior to this, we discuss the user's registration process and how one user subscribes to another user. These two initial steps are of major necessary for all subsequent operations, independent of if reactive or pro-active location-based services at hand.

4.3.1 Message Interactions for User Subscriptions

This section discusses the process how users utilize subscriptions to request location information from other users. In the following three flow diagrams are presented. The description is deliberately implementation independent and rather demonstrates the basic concept.

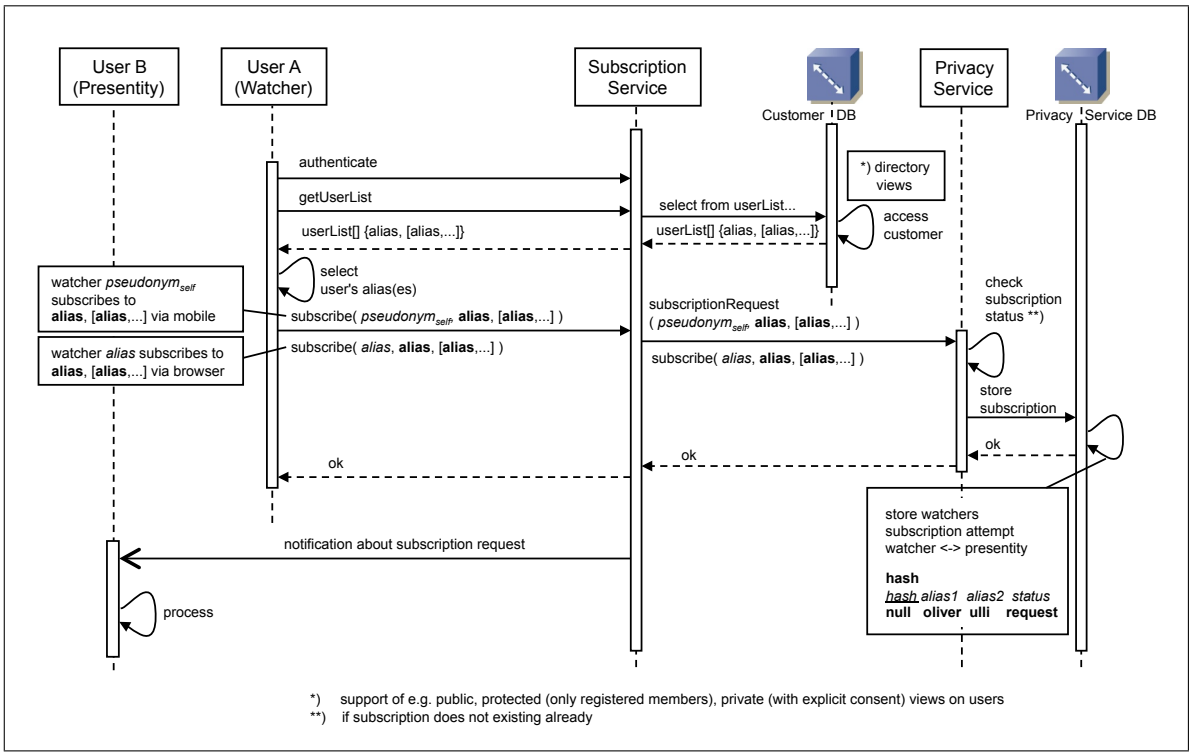

Figure 4.2: User Subscription

Request for Subscription

In figure 4.2 the subscription service as well as the downstream privacy service are depicted on the right side of the picture. Both services are part of the network operators domain and are thus trusted by the users. The left side of the picture shows the watcher and the presentity. Subscriptions are initiated by a user with the objective to get the permission to later request the location information of another user. To receive a list of user's aliases, she first has to authenticate at the network operator's subscription service. Subscription requests are usually submitted via the mobile application. This allows the use of self-identifying pseudonyms for authentication and prevents from additional means for the establishment of a secure link such as e.g. SSL. In figure 4.2 the authentication is depicted by the arrow that is labeled with `authenticate`. The subsequent process of verifying the self-identifying pseudonym is intentionally omitted here. If the subscription service is accessed via web-bowser, the requester cannot provide a self-identifying pseudonym. In this case the user's alias name and the master password that were chosen during the registration procedure are used. This requires additional means to provide a secure communication link such as SSL. The subscription service is also called by the mobile software to initiate the initialization of the user's self-identifying pseudonym. The initialization is initiated when the mobile accesses the subscription service for the very first time. Technically this kind of pseudonym does not differ from the pseudonyms used to express the watcher - presentity relations. Even the algorithms and procedures applied for the generation of these pseudonyms are completely the same. For

the sake of clarity we omit here a detailed discussion about the initialization and generation of pseudonyms. For that we refer to section 4.4.3 (p. 116) where this is discussed in close detail.

As soon as user has successfully authenticated at the subscription service, she may now continue to search and query for other users. Therefore, the subscription service provides some standard masks that, according to the user's preferences, allows to narrow down the search result to a reasonable number of possible candidates. Users may enter the full name or alias, select age limits, gender, languages and possibly groups of interests to name only a few. This functionality is very popular and implemented by many instant messaging systems. As a result, the requester receives a list containing one or several alias names (`userList[]{alias, [alias,...]}`) that correspond to her search attributes. She may now select one or more users and subsequently send the subscription request.

If the subscription request is sent from a mobile device, the corresponding subscription message `subscribe(pseudonym_self, {alias, [alias,...]})` contains the self-identifying pseudonym as first argument. This is followed by a list containing at least one or more aliases of the selected users. To provide message integrity, an additional HMAC is generated for each particular request. This HMAC uses the list of all arguments of the message, that is, the self-identifying pseudonym and the whole list of alias names as input. It guarantees that the message content cannot be altered during transit. To verify this additional HMAC, the privacy service uses the self-identifying pseudonym to first determine the requesters identity. This reveals the shared secret with which the requester generates the additional HMAC and allows to subsequently verify the HMAC. This process is very similar to the verification of digital signatures that use certificates. As the use of HMAC is advantageous in many respects. The most obvious reason is that it does not require much additional computational effort and that it is less complex than digital certificates which require the maintenance of a public key infrastructure. If the request is initiated from a browser, the first argument is the alias name of the requester. The second argument is destined for the alias name of the chosen presentity. If more than one user was selected, the subscription request contains a list of the selected user's aliases instead of a single one.

Next the subscription request is processed by the privacy service which includes a verification of the actual subscription status. This means, if there was no such subscription before, the subscription request is stored. For each received alias name that represents a presentity the corresponding watcher - presentity relation is stored in the database. Optionally, a textual description of the actual subscription status (`request`) is stored and a placeholder for the corresponding hash value (pseudonym) which is at this state set to `null`. Since hash value entries `null` infer the current subscription status `request` it is also possible to omit the field intended for the textual description.

Each change of the subscription state may induce a notification message. A new subscription request may the trigger event to notify each presentity. Another possible way to inform each presentity about pending subscriptions is to await their request. Such requests for subscription states could be performed periodically or once the application is started. Users who access the subscription service via web-browser should also be possible to accept or deny pending subscription requests. Based on their decision the subscription service should be able to either notify the watcher about the acceptance or refusal of a subscription attempt or simply update the state and wait for the next subscription status request from the watcher.

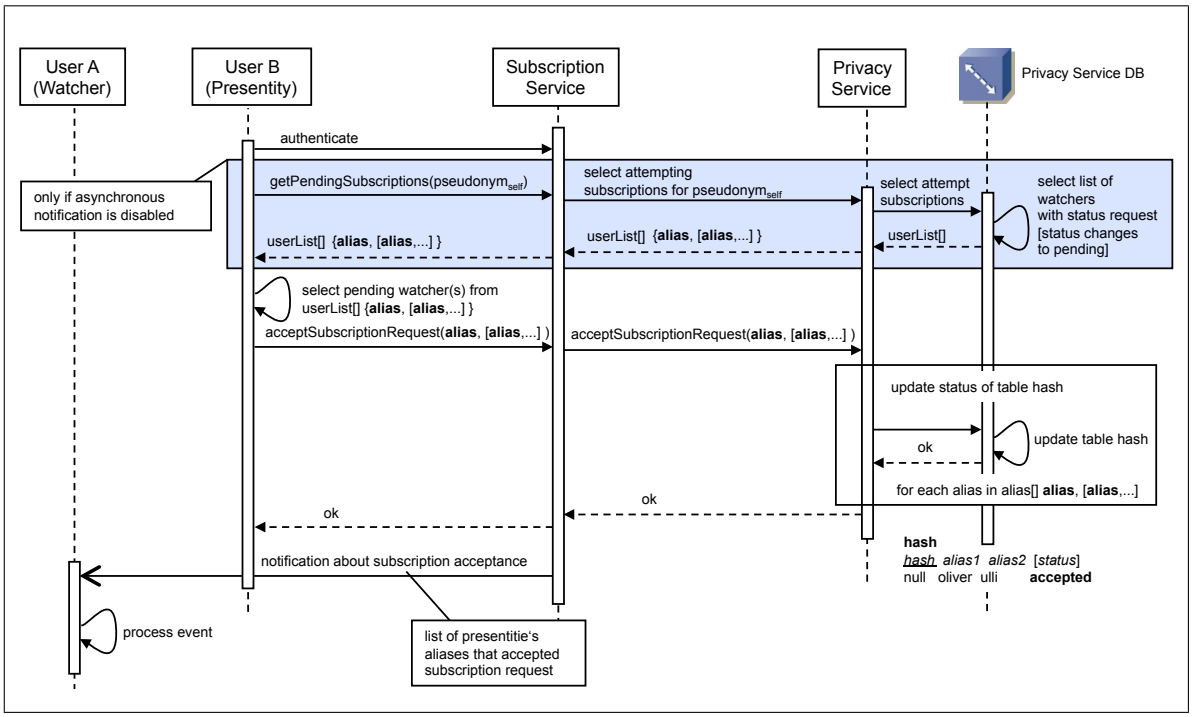

Figure 4.3: Presentity requests and accepts Watcher's Subscription request

Accepting Subscription Requests

The next step of the subscription process is to accept or decline all pending subscription requests. Figure 4.3 further shows the case if the asynchronous notification option is disabled or not available. In this case the presentity has to actively request for pending subscriptions. As shown, message `getPendingSubscriptions(.)` contains a self-identifying pseudonym. The corresponding answer returns a list of those users that are waiting for an acknowledgement. To accept subscriptions the presentity sends message `acceptSubscriptionRequest(.)`. Unwanted subscription requests are declined by the corresponding message `declineSubscription Request(.)`. In this case, the subscription state is either stored permanently to avert further requests from that watcher or the current pending subscription entry is simply deleted. The latter strategy allows a watcher to send a subscription request destined for the same person again. Thus, it is reasonable to provide means that avoid recurring subscription requests within short time periods to prevent from annoying unwanted subscription attempts. One possible way to achieve this is to add a timestamp.

To accept pending subscriptions, the presentity sends the alias names of the respective watchers as part of message `acceptSubscriptionRequest(.)` to the subscription service. Upon receipt, then the privacy service first changes the subscription status from *pending* to *accepted*. Second, the alias name of the user who accepted the subscription request is prepared to be conveyed to the watcher. Now, the watcher is notified about the acceptance of the subscription by user B. As already discussed above, if it is possible to notify the watcher about the subscription change asynchronously, also the respective watcher(s) may in

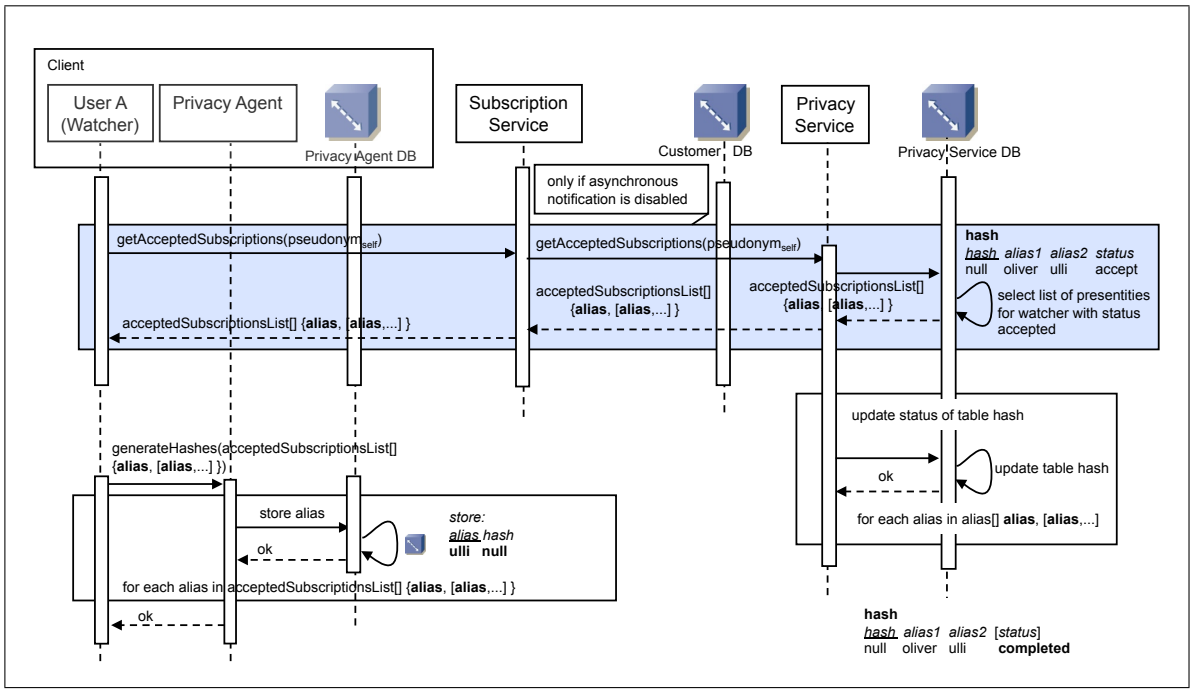

Figure 4.4: Completion of the Subscription Proccess

turn be informed about successful subscription attempt(s). In case asynchronous notification is not activated or possible, users may have to poll for subscription changes. In figure 4.3 message `getPendingSubscriptions(.)` contains the respective self-identifying pseudonym. The privacy service first translates these pseudonyms and returns the respective alias names of those users who attempt to subscribe, `null` otherwhise. Independent of how the actual subscription state was queried (be it by means of asynchronous communication or by polling), if user A's subscription attempt to user B is acknowledged, the respective response contains the alias name(s) that are subsequently used to initialize the hash chain. This initialization is done by the privacy service and by the privacy service likewise. For a detailed discussion on this issue we refer to section 4.4.3 (p. 116).

Subscription Completion

At this stage we can assume that the privacy service has already computed and stored the first pseudonym that associates the particular watcher - presentity relation, namely that of user A and user B. In order to be able to request the location of user B, user A first has to compute the respective pseudonym. Figure 4.4 shows the case when a watcher (User A) receives the list of aliases of those presentities that accepted the subscription requests. This response message contains the associated aliases that are necessary for the computation of the pseudonyms. As user A receives the aliases it first calls `generateHashes(.)`. This call stores the received aliases but does not generate the actual pseudonym as it is done by the privacy service. The reason for that is that the pseudonyms should be computed as recently as they are needed for a service call which prevents storing them in insecure memories. As

the subscription process is now finished, there is however one final remark that should be mentioned here, that is the authentication part. Thus, we discuss the subscription process again in detail in section 4.4.3 (p. 116). There we show that with the introduction of different authenticated shared secrets that are applied to dedicated pseudonym chains we can present an elaborated and secure pseudonym generation scheme. The following section explains the message flows and the pseudonym generation scheme by means of a simple location request.

4.3.2 Message Interactions for a Single Location Request

In the previous section we already explained the details about the subscription process between two users. Now, we show how users can perform a request, that is, how user may request some service that makes use of the location information of that particular other user.

For the following explanations about the message interactions we first review briefly the system architecture. A discussion about the system architecture, its components and the requirements is provided in section 4.1 (p. 91). Instead of that, figure 4.5 shows only the most important components subdivided into several building blocks. This abstract view shows in the center the domain of the network operator which comprises the sum of all network relevant services denoted as *Network Operator Services*. This simple schematic representation subsumes all the services of the network operator, such as the location service, and the privacy service. These are compiled into a single graphical element to simplify the picture and thus allows to better follow the message interactions that are processed for each service request. Since all these services are part of the network operator's domain they are assumed to be trusted by the customers and hence also store sensitive information about each registered user including records about personal data as well as the current position information. For the realization of the proposed pseudonym scheme the network operator also administers the user's pseudonyms and the associated user relationships. Another important block that is under the sole supervision of the network providers domain is the user's device.

In figure 4.5 (p. 107) both users are shown as circles denoted by A and B respectively. User A is the watcher whereas user B is the presentity. Since this scenario discusses the case when user A asks for the location of user B, only the circle that represents user B who is localized is depicted to be part of the network operator's domain. Even though user A is part of the network operator's domain, this arrangement shall point out that in this scenario the network intrinsic localization technology is used.

The block on the top if the triangle represents the 3^{rd} party application provider. As indicated, the service provider may in the simplest case represent a map service that shows the position of a particular user by means of graphical representation. The map itself is generated by a subsequent web service which the service provider has access to.

The two tables on the bottom of the picture show the hash values that are used for each successive service call. Each hash value represents the relationship of two users, as in this case that of user A and user B. One stringent requirement is that the pseudonyms do not get out of sync. If this happens a error recovery procedure is initiated. We describe this procedure in detail in section 4.3.3 (p. 108).

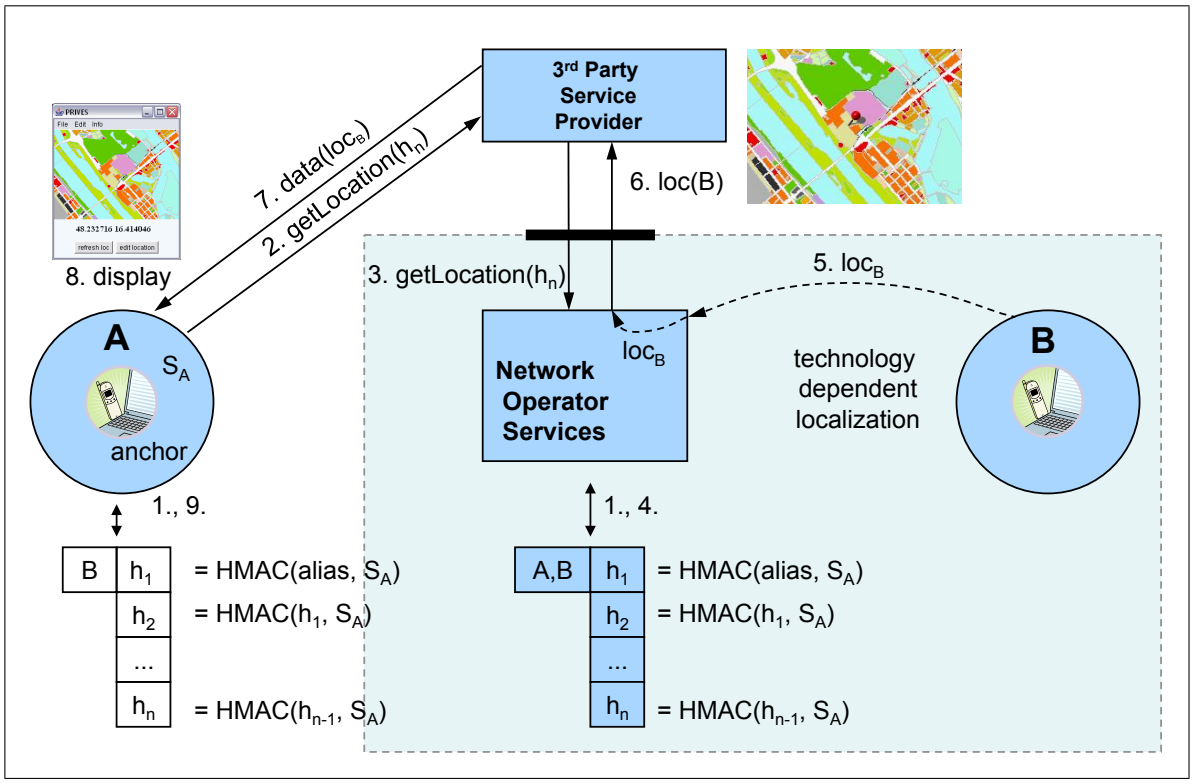

Figure 4.5: Message Interactions according to First Prototype Implementation

Call `getLocation(.)`

This blocking call is the first actual request that is initiated by user A. It initiates a lookup of user B's location and immediately returns the result. Therefore, user A generates the very first pseudonym $p_1 = HMAC(alias, S_A)$ (message 1) sends this as part of the `getLocation(.)` request to the 3^{rd} party application (message 2). The service provider cannot reveal any information nor identity from the pseudonym. It forwards the pseudonym to the network operator's location service (message 3). Now the pseudonym is translated by the privacy service to a unique identifier that can be used by the location service to determine the actual location of user B. The location request (message 5) is shown as dashed line labeled by loc_B. As the location service receives the location of that particular user B from the network operator, the request (message 3) can be processed. Upon receipt of the location the service provider calls a remote WebService that, given a certain cartesian pair of coordinates, returns a map of the surrounding area. The map is further enhanced by a little graphical pin which is mixed into the center of the map to indicate the actual position of the user whose location is asked for. Finally, this map is sent back serialized to the requesting client (last step 8) where it is shown on the screen.

4.3.3 Recovery from Pseudonym Chain Errors

There are some reasons such as fraud or transmission errors why a single hash value and hence the whole hash chain may become out of sync. One such reason that disturbs the pseudonym sequence are multiple requests are submitted in quick succession. As a consequence, delays that are caused by the application due to heavy load or network congestions may be responsible for pseudonyms to arrive in the wrong order. One possible way to overcome this is to buffer received pseudonyms that cannot be validly assigned. Only if a subsequently received pseudonym and thus also all meanwhile buffered pseudonyms can be successfully assigned, the hash chain is restored.

One important thing that has to be considered carefully when pseudonyms shall be buffered in case of one pseudonym cannot be assigned regards the question of the size of such a buffer. What is the optimum size of such a buffer? We believe, that it makes sense to buffer a single pseudonym only. The reason for that is because each additional buffered pseudonym would require users to resubmit another pseudonym. As a consequence, the more pseudonyms are buffered, the more cumbersome the operation of the service becomes for the users.

For example, in case a pseudonym p1 was delayed for some reason and causes another pseudonym p2 to arrive before p1, the pseudonym p2 cannot be verified. So, pseudonym p2 is stored. After that, the first request with p1 arrives. Now p2 is validated and deleted from the buffer. If both requests with p1 and p2 are accidentally of the same type (e.g. `getLocation(.)` both requests are qualified as one. If the requests differ from each other, more complex verifications have to be applied to avoid contradictions. This is not discussed here.

In case a received pseudonym p1 arrives but cannot be verified due to e.g. deliberate modifications during transmission or any other influences, it is at first also buffered. As soon as the following pseudonym p2 cannot be verified too this exceeds the size of the buffer and triggers the re-initialization of the pseudonym chain. It makes no difference, if the received pseudonyms p1 and p2 are of the same pseudonym chain. This cannot be detected. By buffering each unverifiable pseudonym it is guaranteed that in any case the respective successive pseudonym of that particular chain is detected. Instead of waiting for the user to submit another request to initiate the re-initialization, for each unverifiable pseudonym the subscription service may return an error message whereupon the client may autonomously resubmit the next pseudonym. If the second pseudonym can then be verified the pseudonym chain is reconstructed. Otherwise, the re-initializaiton procedure is initialized.

In any case, the detection and correction of errors of pseudonyms does not require much computational overhead, nor does it require much additional bandwidth. Another advantage is that also no further user interaction is needed.

The remarks on pseudonym error detection and verification so far assumed that for each request that contains an unverifiable pseudonym finally the privacy service returns the corresponding error message back to the user. If clients send requests asynchronously, that is, they do not await an OK or error message in case of erroneous pseudonyms, it is much more difficult or even impossible to inform the client. In this case it is the clients responsibility to initiate the re-initialization procedure. It is also up to the client to decide, when a pseudonym was most likely not verifiable. This can be determined by resubmitting the request after a certain time threshold. If the second request does not deliver the expected output, the re-

initialization procedure is initiated. Therefore client A sends a new subscription request for user B to the network operator's subscription service. Then, the subscription service forwards the request to the privacy service where the already existing relation between user A and user B is identified. Hence, as both users have already subscribed, the privacy service generates a new random number and initializes a new hash chain for this particular relationship. The random number is sent back to user A who also initializes a new hash chain for user B. As user A sends the next request, she uses the first hash value of the newly generated hash chain. If no transmission errors occur, the hash chains are consistent again.

Does it make sense to trigger the re-initialization procedure even when no sync errors happened? Does it make sense to call the re-initialization procedure from time to time, or if a certain number of hash value calculations of a particular chain has been reached. Due to the high security level provided by the HMAC construction such re-initializations are basically not necessary. But, in section 4.6 (p. 122) we discuss frequent pseudonym changes and show that this can be also beneficial.

4.3.4 Communication Pattern

The technical discussion about the system and the message interactions showed a rather limited set of commands and interaction possibilities. The reason for that is mainly determined by the exclusive use of synchronous location requests. With so called *blocking calls* each request requires the requester to await the corresponding answer. As the preceding explanations about the recovery procedure of pseudonym chains suggests and in consideration of the varying technical circumstances that come along with the mobile network infrastructure, especially mobile services require sufficient means to allow asynchronous communication. As mobile communication systems are per se characterized by loosely coupled communication links with asynchronous communication patterns for the design and implementation of location-based services that operate on the whole communication stack additional technical means are required. This includes synchronization of various kinds of distributed states, instant notifications upon state changes and solutions to guarantee constant performance and scaleability to name only a few. It is clear that for the development of mobile services this does not only constitute a basic requirement but also a challenge.

4.3.5 Assessment according to the Classification Schemes

Another important question that has to be considered can be derived from different possible classifications as they are discussed in section 2.2.6 (p. 24). The conglomerate of the proposed system architecture, the pseudonym generation scheme and the synchronous communication pattern allows for the development of reactive and position-aware LBS. Reactive because the requester must actively request the location information of another user. Position-awareness is clearly expressed by the role of the requester who simultaneously requests and receives the location information. In the context of the proposed service architecture the definition of location-tracking services may be a bit confusing. In the light of the definition of location-tracking applications where the receiver of the location information may differ from the requester which means that the location information may also be collected and processed by a third party that operates on behalf of the requester, the location platform may be interpreted

as location-tracking system. However, location-tracking is also associated with continuous location updates whereas position-awareness implies location updates on explicit request.

An answer to the question if this example represents a self- or cross referencing LBS provide the pseudonyms. Since each pseudonym represents a dedicated relation between two users in case of self-referencing pseudonyms where the requester and the queried person are the same we can talk of a self-referencing system. If the pseudonym refers to different persons its a matter of cross-referencing LBS. Since many applications allow both, requesting information that is associated with the own position and the location of one or more others, the use of pseudonyms that veil the underlying identities renders the distinction between self- and cross-referencing rather meaningless. However, from the security and privacy protection point of view this distinction is of particular importance.

As cross-referencing already suggests, the number of individuals that can be queried at once is in fact only applicable to location tracking systems. Thus, the so far discussed localization system represents a pure single-target solution.

To sum up we can conclude that the so far presented localization system is reactive, position-aware and self-referencing, meant for single-target use only. We have intentionally not discussed the distinction between in- and outdoor here even though the applied localization technologies are one of the decisive factors of location-based services and applications. For the moment we assume that the location is solely determined by the network operator. This simplifying assumption should not belie in the fact that the different possible localization technologies do not have tremendous influence on the design and maintenance of location-based services. But, for the investigations so far the inclusion of various kinds of localization techniques would have no additional advantage.

4.3.6 What kind of Applications?

Based on the given system configuration, questions like "what kind of applications can be implemented on top of that system?" arise. Furthermore, "are there any systems that provide at least approximately the same set of functions?" and "if, what technology is used for the realization it and how does this technology differ from the one suggested to be used for the proposed system?". At this point we want to mention that the implementation aspects are discussed later in this dissertation and that the focus here is not to explain implementation issues.

One might come to the conclusion that a solution with a functional range similar to the presented solution is rather simple, not to say inadequate as commercial product. Indeed, many commercially offered location-based services do in a sense not provide more functions than those described so far. Such applications include simple friend[5] or car finder [6] applications and make mostly use of existing technologies such as SMS which allows for the realization of asynchronous communication without much implementation costs. Solutions like these are advantageous in many aspects. Due to its simplicity the reusability of almost all existing technologies the implementation efforts and costs are rather low. Another advantage is that the means for localization is provided exclusively by the network operator. As such systems do not provide any means that allow the exchange of sensitive data also legal questions regarding

[5]sniff (social network integrated friend finder): https://www.sniffu.com/ (last viewed 23. Apr. 2009)
[6]A1 Carfinder: http://www.a1.net/business/carfinder (last viewed 23. Apr. 2009)

localization are solely under control of the operator. Another important benefit is that SMS based communication allows such applications to be operated on almost any mobile device and thus potentially every customer. From a security and privacy point of view there are no objections since no privacy sensitive data leaves the network operators domain. Any involved third party provider has to accept the specifications defined by the network operators which reflect legal obligations.

In contrast to these services the presented localization platform which is introduced in the next section requires dedicated software that have to be installed on the mobile devices. The basic operation of this software includes means to manage, store and process pseudonyms. Aside from this basic functions that cover the operations of a privacy agent, this software must also be able to attach or detach software modules and perform configurations according to the respective applications needs. Aside from other modules that implement some basic operations such as e.g. the realization of the graphical representation also application specific tasks and communication means may be required to be dynamically exchangeable. This especially in the case when users frequently attach to various different applications and if this software is then used only for a short period of time. This opens interesting research questions that investigate the possibility how dynamic configuration of software and even dynamic service composition on mobile devices and micro service creation[7] can be achieved. However, this is definitely out of scope of this dissertation.

Finally, one important aspect that this dynamic provides is the ability to upgrade the security of HMAC and thus keep the proposed pseudonym generation scheme up with the highest security requirements. Whereas the security of HMAC and thus the proposed pseudonym generation scheme is out of scope, the introduction of each new MACs which provides higher security should be implemented as soon as possible. With the possibility of dynamic updates of only some parts of the mobile software, it is possible to keep up for secure and up to date means of privacy protection can be can be applied without any needed user intervention.

In section 2.4.9 (p. 61) we discussed the question if it is possible to manipulate software that uses the wireless link. It is clear that the exchange of software modules that are provided by third party application providers may represent a threat to users and network operators likewise. Thus the gainings of the possibility to exchange software and create services dynamically have to be traded carefully with the potential danger that may arise from this.

4.4 Functional Details of the Location Service Platform

The aim of the discussion on the location-service platform so far (see section 4.1 (p. 91)) was to give a general overview of the system architecture, also by referring to the business model viewpoint as it is discussed in section 2.3.3 (p. 42) and the basic system interactions. These explanations point out technical aspects, as such a description of the various components, the pseudonym generation scheme and a description of the system message interactions undertaken for a single location request. In conjunction with the explanations on the proposed pseudonym generation scheme we show how privacy towards the application service providers can be achieved without loss of the user's trust and confidence. The given example shows

[7] m:ciudad: http://www.mciudad-fp7.org (last viewed 23. Apr. 2009)

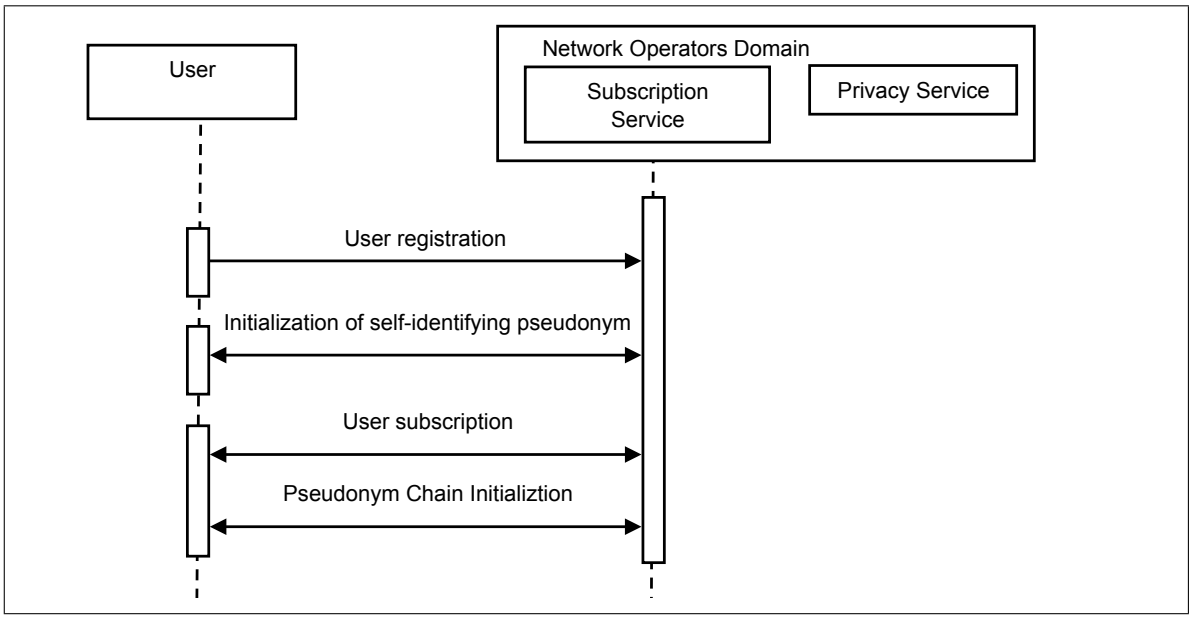

Figure 4.6: Registration, Subscription and Initialization of User's Pseudonym Chain

the basic service operations including in detail the user's subscription procedure as well as message interactions necessary to initiate single location requests. All these descriptions are implementation independent and thus can be implemented with various different technologies. To sum up, the aim of the explanations so far was to give a basic understanding of the system's core construction and communication principles.

In difference to the previous explanations in the following we show certain aspects with the emphasis on additional communication patterns which are essential for the realization of more complex communication patterns than presented so far. We overcome some of the limitations and constraints we identified by comparing with and analyzing the existing location-based services as they are given in section 4.3.5 (p. 109). As a result this allows to implement also complex communication patterns that clearly differ from the previously introduced blocking calls like `getLocation(.)`. The following explanations mainly head for asynchronous communication patterns that constitute the basis for tracking platforms and allows users to interact with the system in a flexible way. Again, all descriptions are intended to be implementation independent.

Figure 4.6 depicts each step of the whole process that starts with the user's registration and the initialization of a self-identifying pseudonym which in turn is used for the generation of user pseudonyms after successful user subscription.

4.4.1 User Registration

The customer's registration process mainly depends on the respective implemented procedures provided and implemented by the network operator's subscription service. In most cases the registration process follows some predefined procedures that include the selection of an alias and a master password. Similar to many other services that are offered by the network

operator, the subscription service accessed by the users during the registration must provide all means that are necessary to exchange and store the sensitive user data securely. As discussed in section 2.4.2 (p. 52), operators are obliged to provide the technical means to meet the legal obligations that shall protect the users data. At this point, we omit further detailed explanations about the protection of any sensitive data at the subscription service which would definitely go beyond the scope of this work. Similarly, we omit explanations on technical details regarding the administration of the alias name chosen by the user and the password. This also includes all means that are necessary to allow users to browse, search and filter users by different attributes.

One important aspect that has to be considered during the registration procedure is that the users must be informed in advance about all the possible consequences that may happen in case of careless handling of their private data. This includes the basically protection of the password, the mobile device itself and also an advice to keep track of access profiles which we will discuss in a latter section. The network operator is not able to take care of the protection of all kinds of personal data (see section 2.4.8 (p. 60)).

As just mentioned above, during the registration process, customers are asked to chose a so called master password. This password can be used for any web-based access to the subscription service to allow users to access and change their personal data or to configure their policies and filters. As with any other web-based system, it is possible to change this master password at any time. Aside from web-based access, the password has also another important function. It serves as an initial shared secret that is used during the initialization of the so called self-identifying hash chain which is administered by the users privacy agent and the privacy service likewise. The following section addresses the issue of how this pseudonym is initialized and what purpose it has.

4.4.2 Initialization of the Self-Identifying Pseudonym

The self-identifying pseudonym is important in two aspects. First, it is significant for operations such as submitting subscription requests or the re-initialization of pseudonym chains in case of an error. Second, with the help of self-identifying pseudonyms the verification of MACs and authentication can be done without the need of digital certificates that require a PKI which has shown to be cumbersome to implement in may cases. Instead of that the use of pseudonyms as proposed in this theses provide an efficient and elegant way to meet the various requirements for secure communication that is otherwise achieved only by applying much more complex cryptographic technologies.

During the registration process the users have chosen an alias name and a master password, which are both stored by the network operator's privacy service. Figure 4.7 shows on the right side the *user data table* that is administered by the privacy service and that contains three columns, one for the user's chosen *alias* name, the second for the *master password* that was initially chosen by the user during the registration procedure which is denoted as S_A which also stands for *shared secret*. The last column contains is reserved for the pseudonym. The table shows the very first pseudonym that is generated with the users alias name and her master password, that is $HMAC(alias, S_A)$.

When the user activates the software on the mobile phone for the first time, it requests for the chosen alias name and the master password. There are several possible ways how this can

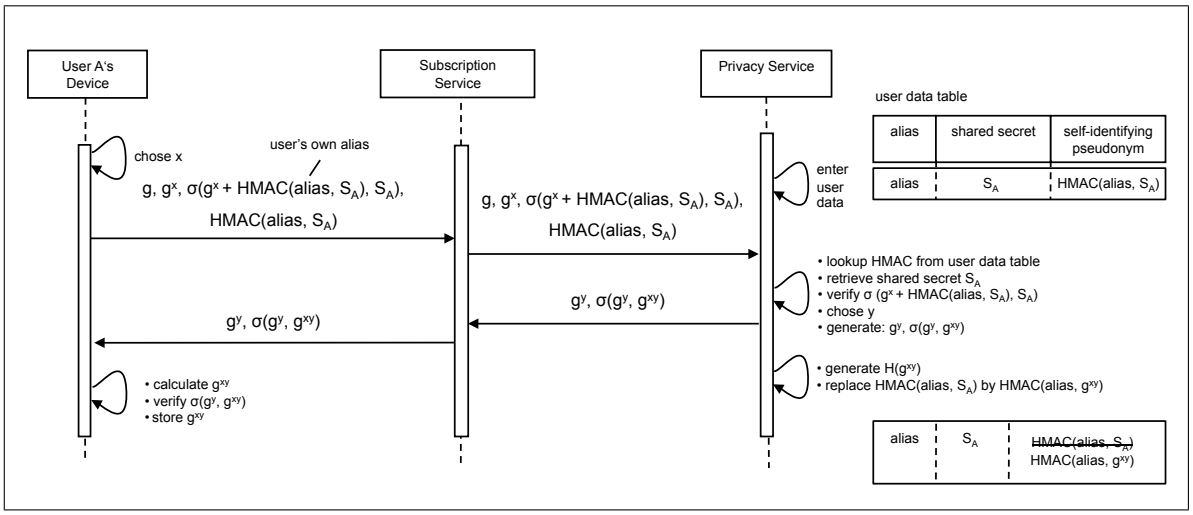

Figure 4.7: Initialization of Self-Identifying Pseudonyms

be achieved. The most simple one is to let the user enter the alias name and master password manually. This requires additional means to guarantee that the entered data is valid before the initialization procedure starts. Another possible way is for the network operator to send the user's alias name and her master password to the mobile phone upon activation. If it can be assured that the communication line during the transmission of the two values stays within the network operators domain, no additional security means are necessary. Regarding the master password it is important to note that this should by no means be stored in the memory of the mobile device. This is reasonable because mobile phones provide by default no means to protect the memory. That is the reason why the password should never be stored permanently on the mobile phone, except when there is a tamper-resistant memory available. Once entered, the master password should also be deleted from the volatile memory soon.

Message Exchange for the Initialization of a self-identifying pseudonym

For the initialization of the self-identifying pseudonym the user's privacy agent first choses a random number which is denoted as x (see figure 4.7). This value represents the private value of the Diffie-Hellman key exchange and is used together with the public value g to generate g^x. This is transmitted as part of the first message. For the sake of clarity we omitted further details of the Diffie-Hellman key exchange protocol and refer to [170]. The first value that is sent by the user's privacy agent as part of the first message is g^x, that is the standard value for the Diffie-Hellman exchange. The second argument is $\sigma(g^x \oplus HMAC(alias, S_A), S_A)$. This MAC contains as input argument the first g^x and the last message parameter $HMAC(alias, S_A)$ that is at the same time the very first pseudonym. This last argument $MAC(alias, S_A)$ is generated by the user with the alias name and the respective shared secret. It allows the privacy service to identify the requesting user, deduce the shared secret S_A and in turn verify the received signature. If the received signature turns out to be valid, the privacy service can be sure that the message was actually sent by the user labeled with *alias* and can proceed with the initialization of the self-identifying pseudonym for that user.

In case of a re-initialization of the self-identifying pseudonym is initiated, the MAC σ further prevents from reply attacks. It even allows for each re-initialization the use of the same initial self-identifying pseudonym $HMAC(alias, S_A)$ for identification. The advantage of this is that for the re-initialization of the self-identifying pseudonym neither the alias nor the master password have to be changed. Anyhow, as explained in the following, each re-initialization generates a completely new hash chain with unique pseusonyms.

With the received g^x from the user's privacy agent the privacy service choses the private value y and generates g^{xy} . With this value, the Diffie-Hellman key exchange is completed. The privacy service hashes the generated Diffie-Hellman secret with the user‘s master password S_A and uses this value to overwrite the initial self-identifying pseudonym $HMAC(alias, S_A)$. The new self-identifying pseudonym is thus $HMAC(g^{xy}, S_A)$.

Now the privacy service continues the Diffie-Hellman key exchange by sending back the value g^y together with the MAC $\sigma(g^y, S_A)$. Upon receipt, the client's privacy agent first verifies the validity of the received MAC. Similar to the privacy service, it then calculates and stores g^{xy} but does not hash this value again. As already mentioned above, the reason for that is the insecure memory of the mobile device. It would not be safe to store $HMAC(g^{xy}, S_A)$ which is already the first self-identifiying pseudonym which the privacy expects for the first operation. It is thus safer to generate each self-identifying pseudonym as it is needed. Furthermore, as a consequence of the insecure memory, it is unwise to store the shared secret S_A permanently on the mobile phone.

Thus, whereas the privacy service stores the $(n+1)^{st}$ self-identifying pseudonym, the users privacy agent stores only the respective previous one, that is the n^{th} one. Each single subsequent request requires in advance the generation of the respective next pseudonym, that is the $(n+1)^{st}$. For that, the users master password is required. The safest way to provide this master password to the application is to require the user to enter it manually. Depending on the respective implemented security policy it is also possible to design the client software in such way that the user has to enter the master password only at least once when the application is started. In this case the shared secret is stored at least as long as the application is running in the volatile memory but not necessarily persistently. This would be a vastly greater security flaw since, as already discussed, most mobile devices do not provide means for secure data storage. There is certainly a trade off between the security and the usability of the system. But, we think that if the user is required to enter her password once the application is started, this may not be to cumbersome to users and on the side enhance the trust and confidence in the application.

In case a re-initialization of the self-identifying pseudonym, the whole procedure is repeated. Since each time the privacy agent generates a random private value x also σ is different. Thus, $HMAC(alias, S_A)$ can be reused as initial self-identifying pseudonym. As all the following self-identifying pseudonyms use the Diffie-Hellman key g^{xy} as input, a unique hash chain is constructed.

4.4.3 Initialization of a Pseudonym Chain

After the initialization of the self-identifying pseudonym, the user may now continue to subscribe to other users and hence initialize a new pseudonym chain that exclusively represents the relationship between this user and the subscribed user. The subscription process involves a number of steps such as search and contact other users to request permission and hence the generation of pseudonyms. At this point we refer to section 4.3.1 (p. 101) where we discuss all message interactions that are part of the subscription process in detail.

One important part for the generation of each pseudonym is the shared secret that is used in each case. Regarding this, there are basically two possible ways how pseudonyms can be generated. The first one is to use the user's master password. Since the master password is already known by both entities, the user and the network operator's privacy service, this way of pseudonym generation is the most easiest one. Another way is to generate shared secrets for each pseudonym chain. The following explanations will show, how this is achieved.

The initialization procedure of pseudonyms is shown in figure 4.8. At a first glance, the protocol is very similar to the one used for the initialization of self-identifying pseudonyms that is described in section 4.4.2 (p. 113). It also uses as first parameter g which represents the public value of the Diffie-Hellman protocol, x the private value. There are some slight differences. When the user sends the first message of the initialization procedure to the subscription service, she provides her self-identifying pseudonym. This pseudonym is also used for the generation of σ. Another difference represents the alias. Whereas the self-identifying pseudonym requires to provide the alias name of the requester herself, this time the alias represents the user for whom the pseudonym is requested for.

Eventually, message $g, g^x, alias, \sigma(g^x \oplus, p_{self}), p_{self}$ is processed by the privacy service. It first verifies the correctness of the self-identifying pseudonym p_{self}. If it is valid, it continues to verify the MAC σ which requires both g^x and the $alias$. Next, it choses a random number y that represents the Diffie-Hellman private key to generate g^y. This is hashed with the newly generated Diffie-Hellman shared secret g^{xy} which results in $\sigma g^y, g^{xy}$. The privacy service returns the newly generated parameters as part of the message $g^y, \sigma(g^y, g^{xy})$ and continues to calculate the respective next self-identifying pseudonym $p_{self} + 1 = HMAC(p_{self}, S_A)$ which requires the user's master password S_A. Finally, the privacy service computes the first pseudonym $p_1 = HMAC(alias, p^{xy})$ and stores it.

4.4.4 Client Initiates First Service Call

When the client receives $g^y, \sigma(g^y, g^{xy})$ from the network operator it first uses x and g^y to generate the new shared secret g^{xy}. This allows it to further verify σ. The newly generated shared secret is now used for the following calculations of the pseudonyms of that chain. The newly generated shared secret g^{xy} should by no means be stored persistently on the client.

The second last command that is executed by the client (see figure 4.8) shows the generation of the first pseudonym p_1. The used shared secret g^{xy} is retrieved from the volatile memory. The following command `getLocation(.)` uses the newly generated pseudonym as argument. Alike the shared secrets of every hash chain, also the generated pseudonyms should be stored in the volatile memory only.

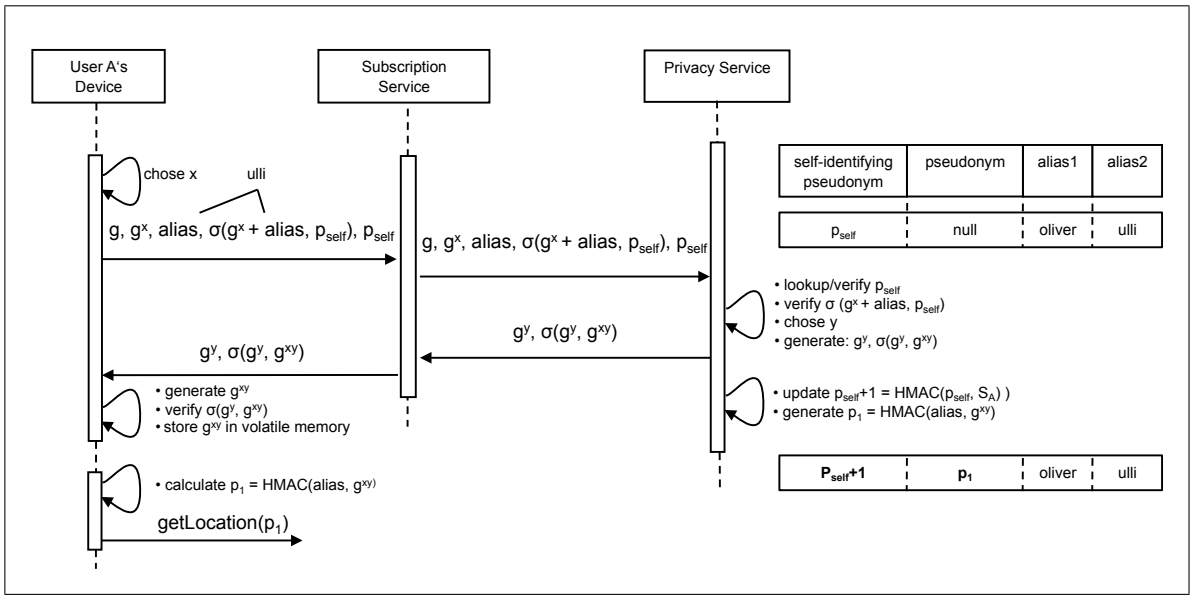

Figure 4.8: Initialization of Pseudonyms

4.4.5 User Submits Single Location Request

In this subsection we continue the above discussion with requests that are initiated by the client to ask for the location of one particular user that is possibly even herself, or the location of several users. In fact, we already discussed this type of request in section 4.3.2 (p. 106). But, wereas there the aim was to show the interworking and connection of the proposed system architecture with the pseudonym generation scheme the focus here is rather on technical aspects.

Figure 4.9 shows how the client first issues a `getLocation(.)` request that contains at least one or several pseudonyms. As there is no difference if the pseudonyms denote the requester herself or any other of the users, here the pseudonyms are simply denoted as `h`. Eventually the request is processed by the privacy service which, upon receipt, translates pseudonyms into the respective identifiers. Given these identifiers the location service may access the location of each particular user. The simplified database scheme in the right corner of the figure highlights a single row which represents the exemplary user whose location is currently asked for. In case the location information of this user is available, it is returned to the user who still awaits the response. The dashed messages signify the answers that may contain the location information in form of coordinates. Finally, the received coordinates are assigned to the respective selected users.

4.4.6 User-initiated Location Update

Another very important operation that is provided by many localization and tracking platforms is to allow users to update and publish their actual location. The increasing deployment of mobile devices that provide the ability to determine their location requires additional functions to allow users to control their location by publishing it. Thus, in this subsection we

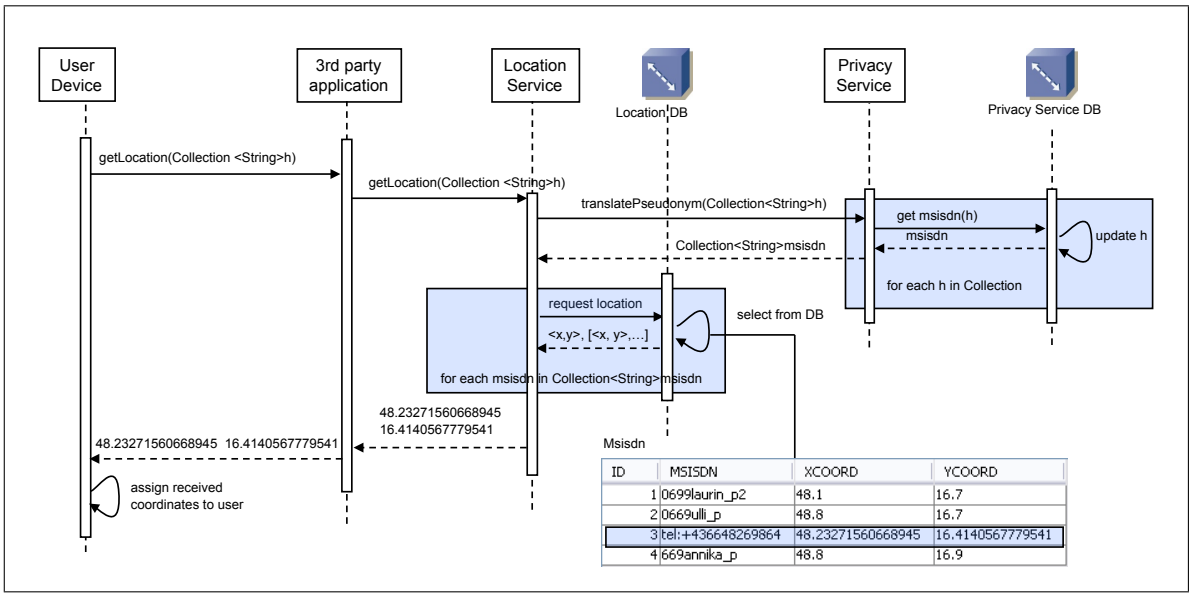

Figure 4.9: Blocking `getLocation(.)` Request

describe the case of a mobile device that has the capability to determine its own position and allows to send this information to the network operator's location service. Figure 4.10 (p. 119) shows the involved entities that are required for this kind of operation.

A location update message `updateLocation(.)` basically provides three parameters. The first one is the self-identifying pseudonym which allows to assign the following coordinate pair that is denoted as `x` and `y`, the second and third argument respectively. Regarding the second argument that contains the actual location information we want to note that the actual location information passed by the users should not be restricted to discrete coordinate pairs only. One essential part that reflects the flexibility of the location service and thus the system as a whole is the realization of proper measures that allow the location service to not only process discrete location coordinates as it is shown here but also to receive, interpret and process descriptive location information. Examples for this includes e.g. location information such as *home*, *work* or even *underway*. Different kinds of such locations are conceivable and further discussed in detail as very important design aspect of the location service in section 4.1 (p. 91).

Another important design decision is whether the location update message is to be sent directly to the location service or not, or in other words, should the location update message be routed through the application? Even though there are no technical barriers for either case, the distinction between these two different kinds of location updates is important. The reason why we route location update messages through the application is because we assume that each service provider has some contractual relationships with a number of dedicated network service providers. We discuss in section 4.7.1 (p. 126) design issues and how location-based services and applications interact across different domains.

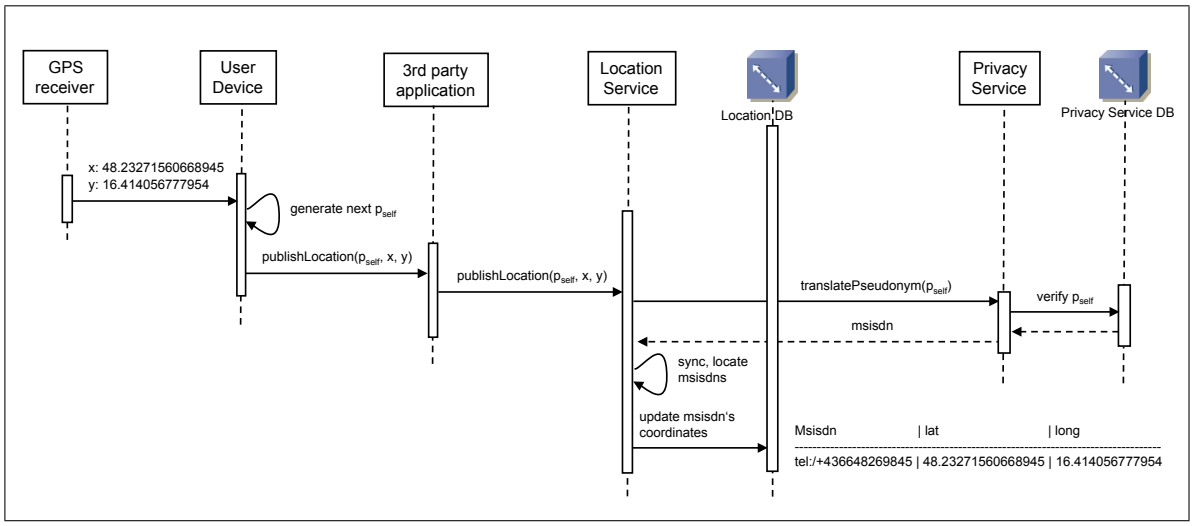

Figure 4.10: User Initiates Location Update with GPS Coordinates

Message Interactions

For the following explanations refer to the use of GPS. The reason for that is that GPS enabled devices are already available for many mobile devices and thus even represent some kind of generality. For an overview on some of the most important currently existing localization technologies we refer to the discussion given in S section 2.2.5 (p. 19).

We assume, that the user's device receives (or determines) its current position. Independent of the used localization method or location format there is the question how often the user's device shall send location updates? Does it make sense if users permanently send their location updates even when they do not move? When is it absolutely necessary or useful to send location updates? At this point we do not want to go into further detail and deliberately omit privacy questions that certainly arise in the context of location accuracy and freshness of available location information. For discussions on this we refer to section 5.7.1 (p. 143) where different kinds of client update strategies are discussed in closer detail.

Before the location information is transmitted, the user's privacy agent calculates a self-identifying pseudonym which is then sent as part of the `updateLocation(.)` command to the application. Upon receipt the service provider forwards the data to the network operator's location service. The following message `translatePseuodnym(.)` contains the self-identifying pseudonym which is translated by the privacy service into the respective unique identifier that is in this example the MSISDN. This is sent back to the location service whereupon the identifiers and the corresponding location data is updated. If the location service is not part of the trusted network operators domain, the MSISDN cannot be used. In this case the privacy service additionally has to map the current MSISDN to another anonymized identifier which can be conveyed without privacy concerns.

The table depicted in figure 4.10 shows the user's identifier that is in this example the MSISDN and its actual position in terms of coordinates. Again, the representation of the database scheme is rather simple and should be understood as a guideline.

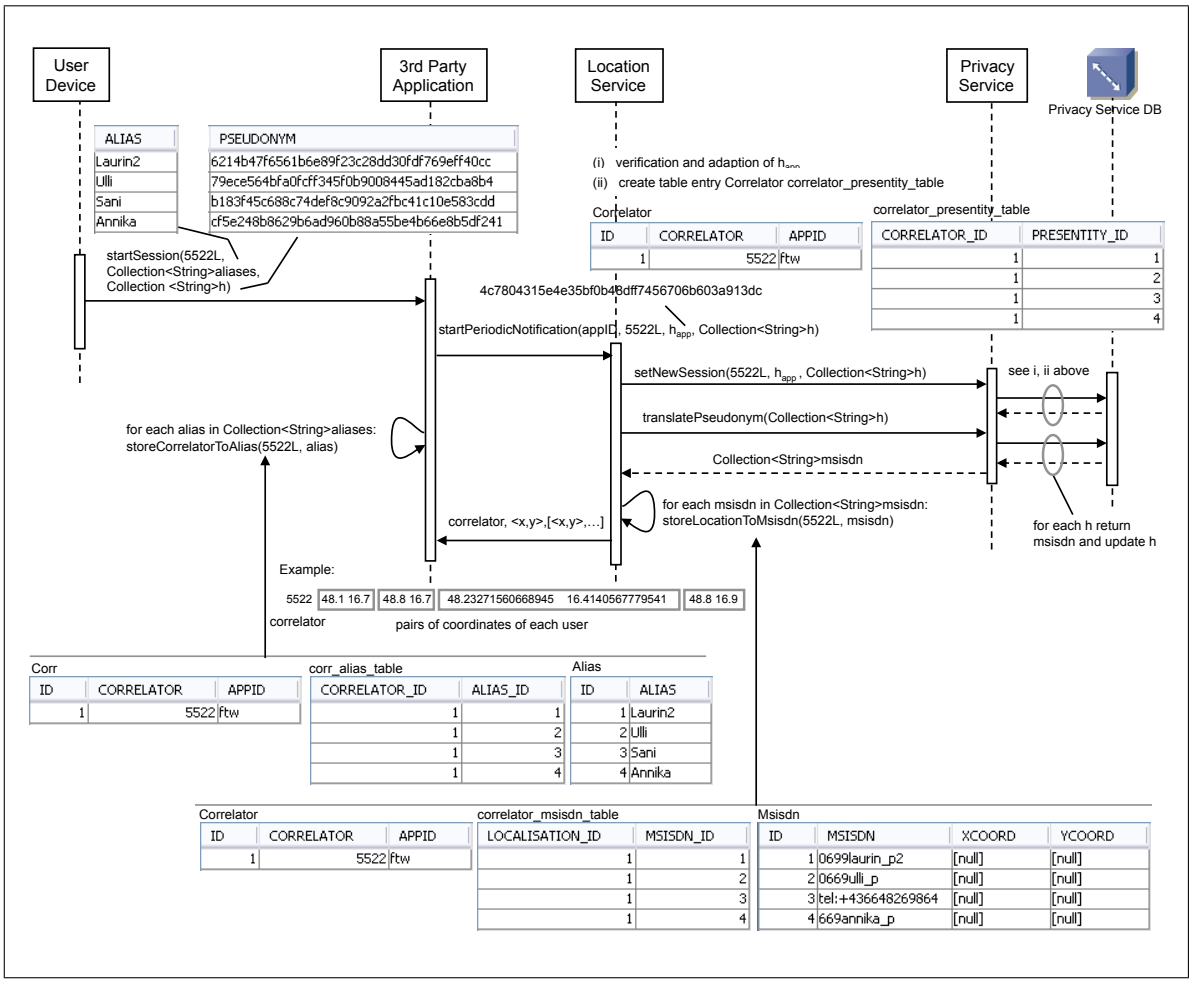

Figure 4.11: Start of Periodic Notification Process with Correlator 5522

4.5 Administration of Long-term Localizations

In the previous section we already gave an outlook how pseudonyms are used to request the location of one or more users. From the discussion so far it is clear that this kind of interaction with the system allows only for implementation of a subset of location-based services and applications (see section 4.3.5 (p. 109)), namely those, which allow single location requests only. Thus, in the following we discuss how pseudonyms are used to provide users the ability to, depending on the respective location-based application at hand, administer even long-term tracking sessions that do not necessarily rely on continuously user interaction. This is challenging in many aspects. One is that it enables the development of a variety of location-based applications. Another challenge is rather of technical nature since since we show that the proposed pseudonym generation scheme can also be applied for this category of location-based services. In the following, we analyze in particular the system interactions and consider the processing of pseudonyms and session management.

Initiation of Long-term Localizations

The first message is initiated by the user. Therefore she selects one or several buddies from the buddy-list (optionally including herself) and pushes a button to activate a new tracking session. Thereupon, the underlying mobile software calculates the respective pseudonyms of the selected users and sets up the message as it is shown in figure 4.11. As described in the previous section, there are two different kinds of pseudonyms to consider. One is the so called self-identifying pseudonym, the second type refers to a particular user we call presentity. Independent of which pseudonym is generated, it is further important if the pseudonym is generated for the first time or not. In the first case the whole initialization procedure as it is described in section and has to be executed. In the second case, the client has to access the pseudonym that was submitted before together with the associated password. All passwords, including the user's master password and the passwords that are used for particular hash chains shall be stored only in the volatile memory of the mobile. They are only accessible as long as the application is activated and deleted as soon as the application is switched off.

The example depicted in figure 4.11 shows a long-term localization process that is started for four persons, namely *Laurin2*, *Ulli*, *Sani* and *Annika*. The command `startSession(.)` contains a so called `correlator` which has the value `5522L`. This correlator represents the session identifier. For the sake of simplicity in this example the depicted correlator is only a simple number. In order to avoid collisions with other correlators that are submitted by other users and processed at the same time, the correlator should be a hash value that uses as input the submitted list of pseudonyms. As each pseudonym is random, the hashing of these values again results in random values that avoid collisions with other correlators with high probability. Alternatively, it is also conceivable to disallow clients to decide which correlator to use for a new tracking session. However, this requires not only to generate a unique correlator at the privacy service but also requires that this correlator does not collide with other existing correlators that are possibly already processed by some service providers that operate in other network operator's domains.

Depending on the respective application at hand the first service call may also contain a list of alias names of the respective buddies. The use of alias names is advantageous in the case when the application shall provide the position of several persons at the same time. The user's alias names can then be used to indicate e.g. on a map, the position of the buddies. In contrast to requests that provide only pseudonyms, this may decrease the high privacy level. But, there are many applications that would make no sense at all if absolutely no additional information such as the alias name is available. Since the client may send the alias names on purpose, it is possible that the application only stores the `correlator`s and the associated `correlator_id`s of active sessions. In this case, the involved users are totally anonymous towards the application.

As the application receives the request, it generates the next application pseudonym h_{app} and forwards this together with the data that was previously received from the user as part of the message `startPeriodicNotification(.)` to the location service. The application pseudonym comparable with the self-identifying pseudonyms of the user. In the case of the application's hash h_{app} we could also speak in terms of the application's self-identifying pseudonym. The location service calls `setNewSession()` of the privacy service which first checks the application's pseudonym and thereafter each user pseudonym. If all pseudonyms

can be verified, a new session is entered in the session table. The privacy service registers the correlator in the table `Correlator` and connects the identified presentities to that session with the help of table `correlator_presentity_table`. The table entries show four users with `PRESENTITY_ID` that are bound to session `5522L`. Next, the location service requests for the translation of each of the received presentity pseudonyms. The privacy service returns the respective identifiers that are necessary for the subsequent localizations. For the sake of clarity we indicate this identifier as to be the MSISDN. But this is not the default case and is meant to be implementation independent. Similarly to the privacy service, the location service creates a new record in a dedicated database table which allows to store the new session. Here, this table is shown on the bottom of figure 4.11 and denoted `correlator_msisdn_table`. Compared to the privacy service, this time the correlator is not coupled with the presentities pseudonyms but with the users identifiers, namely the MSISDNs or any other other possible unique identifiers. Regardless of whether the location service is part of the network operators domain or not, the identifiers that are used by the service providers to denote the users (`alias`) and the identifier used by the location service (`msisdn`) are associated by their order. This is important when the location information of all users of a particular session are sent to the service provider. The last message in figure 4.11 shows the message contains the session identifier (`5522`) and four pairs of coordinates of users, namely that of *Laurin2*, *Ulli*, *Sani* and *Annika*.

The discussion so far considered only the case where users are within one single domain. It is however also necessary to analyze the case when location-based applications that are operated in completely different areas access operator's services that reside in different domains and thus provide different kinds of location-based services. The following discussion is dedicated to this very important issue.

4.6 Pseudonyms with respect to *Off-the-Record* Messaging

The idea to digitally sign the Diffie-Hellman exchange parameters is proposed by Borisov et al. [15, 171]. In contrast to our variant solution which rather focuses on the generation, processing and communication of pseudonyms, they solution provides means for the establishment of shared secrets that primarily allows for privacy preserving communication which is, as they argue, an important prerequisite for social communication. In other words, their aim is to allow users to communicate in a way that is close to real-world conversations which differs from traditional security means such as they are provided with PGP, SSL or S/MIME that are commonly used.

From a more technical viewpoint, their solution for the realization of close to real-wold conversation or as they call it *Off-the-Record Messaging* (OTRM) provides means that allow *perfect forward secrecy* (see section 4.6.3 (p. 124)) which is important to protect from future compromises. However, at a first glance their proposal to use digital certificates for user *authentication* seems to be a clear contradiction to the required *repudiability* that is another important property to private communication[8].

In the following, we will discuss how Borisov et al. manage to overcome this contradiction

[8] A detailed description of *Cryptographic Primitives* is given in section 3.2 (p. 79). For an overview about *Security Services* we refer to section 3.2 (p. 79)

and analyze the similarities but also the differences of our solution used for the initialization of self-identifiying pseudonyms. In doing so, we compare our approach with the OTRM approach and discuss the interpretations of *perfect forward secrecy*, and security services such as *confidentiality*, *authentication* and *repudiability*.

4.6.1 Authentication

The discussion starts with what is actually achieved by signing the initial Diffie-Hellman exchange parameters g^x and g^y. Therefore, we first have to clarify that we do not use the notion of digital signatures in the sense of public key cryptography. The kind of signature we use is rather based on HMAC calculations. But, similarly to public key signatures, the use of HMAC allows to provide *data integrity* and message *authenticity*.

Thus, we use HMAC in two different ways. The first one refers to the generation of pseudonyms, be it self-identifying or any other. Second, HMACs as signatures. In the following if we use the term signature we mean those that are based on HMAC. Alike Borisov et al. [15] we do not sign the whole message. Instead of that we also sign only the the Diffie-Hellman exchange parameters.

But what is the difference between these two kinds of signatures and why do we propose the use of signatures that are based on HMAC? Lets first review the differences. Signatures with certificates allow any receiver of a message to identify the author. In contrast to that, HMAC based signatures are totally anonymous towards anyone except for the privacy service. Borisov et al. [15] argue that they do not use signatures to prove the authorship of *whole messages*. Instead, they acknowledge that anyone may know who chose the value of x that is used for the transmitted g^x. This means, that the use of signatures that include certificates enables any receiver of that message to identify and verify the respective authorship.

As each signature is only a matter of Diffie-Hellman exchange parameters which, as Borisov et al. refer to, does not have anything to do with the *whole message* - that is in our case the resulting pseudonym, it would make no difference if we would generate signatures with certificates. Thus, the only reason why we prefer the use of HMAC signatures is that is leaves out the complexity that originates through the inclusion of a PKI. But, there are also other reasons for the use of HMAC signatures which are indeed less significant but important to be mentioned. One is that we do not need to prove authorship of Diffie-Hellman exchange parameters towards anyone else than the privacy service. Since the initial HMAC is generated by means of the alias and the master password that was chosen by the user during the registration phase, the resulting MAC it is not only sufficiently distinguishable from all other MACs that are administered at the time by the privacy service but further provides enough security that prevents from any possibility to unintentionally reveal identity information. It is obvious that there is no need to prove authorship to anyone else than the privacy service nor do we need to authenticate even Diffie-Hellman exchange messages to anyone else than the privacy service. In fact, we require quite the opposite that is *anonymity* towards 3^{rd} party application providers. Thus, as one stringent requirement that also stems from the system architecture and involves any message including the Diffie-Hellman exchange messages is that the only entity that may authenticate the authorship of messages is privacy service. From this follows that as we only need to prove identities towards service providers. Thus, any signature system that allows to prove message authenticity towards any other entity that the

privacy service represents a contradiction to our requirements. Thus, it turns out that only HMAC signatures fit our requirements best and are thus in favour.

4.6.2 Repudiability

The reason why we also discuss repudiability in association with the initialization and generation of self-identifying pseudonyms lies in the fact that, as already mentioned above in the course of the discussion about authentication, both, self-identifying pseudonyms and OTRM are subject to the same principle mechanisms that lead to repudiability.

If we review OTRM, here repudiability as one basic principle of close to social communication means that it should not be possible to prove that a message was really sent by one party, independently of whether this is true or not. Not less important, in OTRM the use of MACs allows the receiver to verify the authenticity and integrity of any received messages. In this connection we talk about signatures that are generated with the help of MACs. By the same token, we achieve authenticity by the use of (self-identifying) pseudonyms.

As a result of the discussion above so far, Borisov et al. state in [15] that because MACs cannot provide non-repudiation it is perfect for OTRM since neither no one else but the privacy service can prove or even determine the sender of a message, nor can the privacy service prove to anyone else that the received message was sent by a particular user.

Similarly to this, the use of pseudonyms on the one hand allows to prove authorship of messages to the privacy service and, what is important to be pointed out, only to the privacy service. On the other hand, pseudonyms do not provide non-repudiation. The important insight of this is that this further implies that there is no way to actually prove the existence of any pseudonym to anyone. This holds in any case, also for all previous pseudonyms in a chain and in case the shared secret of a chain is discarded and replaced by another one. Thus, it makes no sense to store any pseudonym nor is it possible to even prove their existence.

4.6.3 Re-keying and forward-security

Another interesting question that arises with the use of MACs applied as signatures and pseudonyms concerns the respective shared secret. In particular, the question is how often the shared secret of a hash chain should be changed. Or, is it necessary to change shared secrets of hash chains et all? Every new shared secret is generated according to the same scheme that is already described above in the course of initializing self-identifying pseudonyms. But, how expensive is the Diffie-Hellman key exchange in terms of the required computational effort and network bandwidth that is required for the message exchanges? As the authors of the paper about *Off-the-Record Messaging* Borisov et al. [15] allude, with changes of the shared secrets the computational overhead of the Diffie-Hellman key exchange is still affordable and does not consume much computing power from the mobile device, neither does it affect the available network bandwidth. However, we indicate that they do not provide any prove or results from measurements.

They further suggest to change the shared secret as often as possible, in the ideal case, even for each new pseudonym that is to be generated for each new message. The underlying reason is that they need the shared secret to encrypt messages. In order to best possible support forward security it is obvious that the more often the key changes, the better forward-security

can be achieved. As we do not use the shared secrets for message encryption but instead of that for the generation of pseudonyms (in fact the pseudonym(s) is one of the most important component(s) of the message), the security property of HMAC supports also the use of long-lived keys which renders frequent re-keying rather useless.

Furthermore, many user interactions such as those that involve the management of tracking sessions do not require frequent user interactions, the additional generation of a new key for each pseudonym would not be too costly. This is an example where the effort of re-keying for each new pseudonym is absolutely conceivable. We denote this case as *just-in-time re-keying*.

However, even if just-in-time re-keying is effective, it is still questionable if it is really advantageous and as such makes sense at all? From a security point of view it makes no difference if the shared secret is changed frequently or not. As discussed in section 3.1.5 (p. 77) on the security of HMAC it is almost impossible to find collisions of the underlying hash function with random secret initial values (that are the shared secrets). Therefore, as long as the shared secret is kept secret for the generation of pseudonyms frequent changes are unnecessary.

4.6.4 Assuring Confidentiality

One of the most important requirements for secure communication is confidentiality. However, as in our case, where no content has to be transmitted and information is at best protected against forgery, additional means for the realization of message confidentiality are unnecessary. The most important information that has to be hidden are the identities of the requester and all other associated users. As this is solely achieved by the use of pseudonyms and this is discussed as far as possible in the course of this discussion, we do only point to the thorough applicability of pseudonyms in terms of location privacy protection.

4.7 Location-Based Services Usage across different Network Domains

This Chapter has been partly published as: [9] O. Jorns, G. Quichmayr, and O. Jung. A Privacy Enhancing Mechanism based on Pseudonyms for Identity Protection in Location-Based Services. In *Australasian Information Security Workshop (Privacy Enhancing Technologies) AISW-PET2007 at the Australasian Computer Science Conference in Ballerat, Victoria, Australia*, 2007.

In the introduction we discussed legal obligations which clearly show the importance of privacy with regard to location-based services and in succession the technological requirements necessary to build stable solutions. So far we assumed that all involved parties such as the users and the 3^{rd} party application providers have a contractual relationship with only one particular network operator. The proposed privacy enhancing mechanism constitutes a good solution with regard to the technical conditions imposed by the clients' hardware capabilities and the privacy requirements that are associated with the use of location-based services and the exchange of privacy sensitive information in general and location information in particular. But, the notion of privacy gains even more importance if sensitive data shall be exchanged

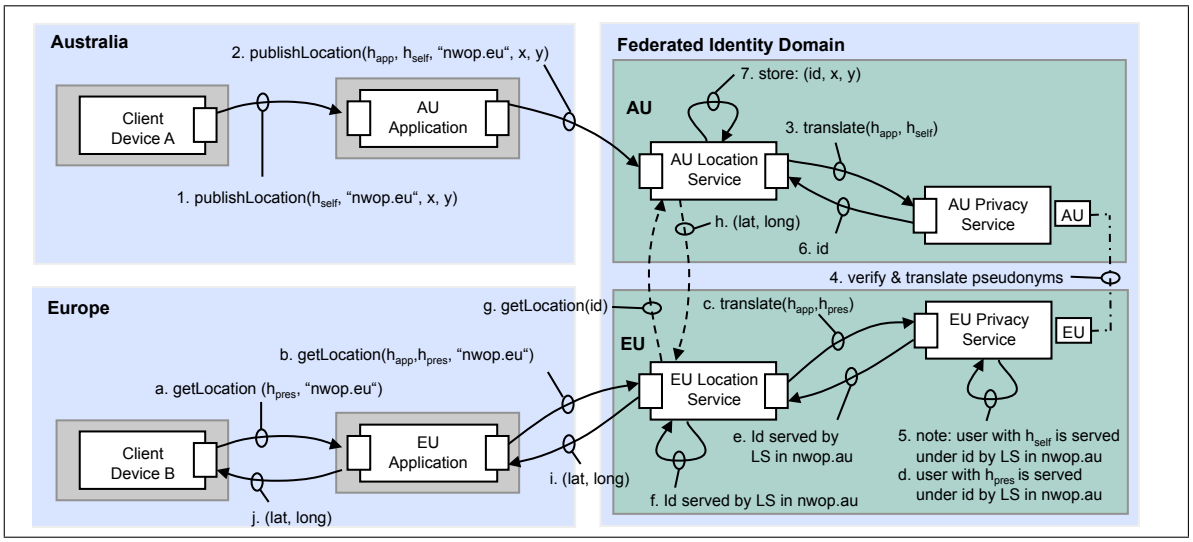

Figure 4.12: Management of Identities Maintained in Different Domains [9]

between 3^{rd} party application providers and network operators of different domains. An attempt in this direction was proposed by OMA (Open Mobile Alliance) (see section 2.4.3 p. 55). It describes how visited operators may push tourist information to roamers. It does however not cover some fundamental aspects of location-based services such as questions concerning the possibility to allow users to update their position.

Our solution refers to O. Jorns et al. [9] and addresses the aforementioned deficiencies. We show, that with only minor extensions, our pseudonym based privacy enhancing mechanism allows for the secure exchange of sensitive data between network operators even when they are located in different domains.

4.7.1 System Architecture View

Each user as well as each 3^{rd} party application provider disposes of a contractual relationship with at least one network operator. The architectural challenge is a solution that allows users to exchange location information under the assumption that at least one user is roaming or even both users have contractual relationships to different network operators. In any case, the system provides the ability to exchange location information across different domains without the loss of privacy.

Figure 4.12 shows the proposed architecture. Compared to the system architecture depicted in figure 4.1 (p. 93). this time several network operators located in different geographical areas provide their services to application providers. For the sake of clarity the following explanations refer to only two different network operators and applications.

Clients may directly access 3^{rd} party applications, no matter to which network the user is connected to. In order to be able to receive location information from users our architecture allows the recognition and translation of pseudonyms even over different service provider specific identity domains. This is archived through a virtual identity domain which passes assertions between the service providers. Compared to the definition of an identity domain

of Jøsang [172, 173] where each identity in an identity domain is unique, we distinguish each domain rather by the respective network operator.

It is difficult to map our solution to commonly known identity management architectures. The used identifiers do not only represent identifiers but are at the same time the credentials used for verification. As the credentials are included in the identifiers or pseudonym they can also be denoted as kind of "*self verifying identifiers*".

For the inter-domain exchange of location data we chose a centralised identity management architecture. Pseudonyms that are used in the visited domain are always forwarded to the home domain of the presentity for verification. The verification process is a simple matching procedure. If the pseudonym can not be found within the set of active pseudonyms this indicates either an unauthorized access or a synchronization error of the HMAC chain has occurred. In case of non matching pseudonyms an error notification is send back to the originator of the associated message which may then initiate the re-initialisation of the HMAC chain. In the following we describe the message interactions for a simple example. Here, one user equipped with device A asks for the location of another user carrying device B whereby user A roames in a different network.

Publish location across different domains

User A is located in the AU domain and wants to publish her current location. Therefore she sends her self identifying pseudonym h_{self} together with the coordinates received from the GPS module to the AU 3^{rd} party application (message 1. `publishLocation(`h_{self}`, "privacy.eu", x, y)`). Now, the AU application generates the next self identifying hash value h_{app} and sends it as part of the second message (`(`h_{app}`, `h_{self}`, "privacy.eu", x ,y)` to the AU location service which in turn forwards only the pseudonyms to the AU privacy service (message 3. `translate(`h_{app}`,`h_{self}`, "privacy.eu")`. If h_{app} is valid, the next step is the verification and translation of the user's pseudonym h_{self}. Since A's home network operator is located in the EU domain, the AU privacy service cannot verify and translate h_{self}. The users' home domain `"privacy.eu"` allows the AU privacy service to contact the EU privacy service (message 4.) which eventually verifies h_{self} and notes that user A is now served by the location service located in the domain of AU (message 5). The AU privacy service receives the identifier `id` from the EU privacy service and sends this to the AU location service (message 6) where it is stored in association the users' location (message 7. `store(id, x, y)`).

Location Query

The transparent use of pseudonyms allows user `B` to query the location of user `A`. Thereby it is irrelevant in which network domain each client is.

As depicted in figure 4.12, user `B` sends message a. `getLocation(`h_{pres}`)` to the EU application which forwards the contained pseudonym together with its self-identifying pseudonym h_{app} and the domain information `"privacy.eu"` to the EU location service (message b. `getLocation(`h_{app}`, `h_{pres}`, "privacy.eu")`). The EU location service requests the verification of the applications' hash value and the translation of the presentities' pseudonym from the EU privacy service by message c. (`translate(`h_{app}`, `h_{pres}`, "privacy.eu")`). After successful verification the result of the translation is returned to the EU location service. Since

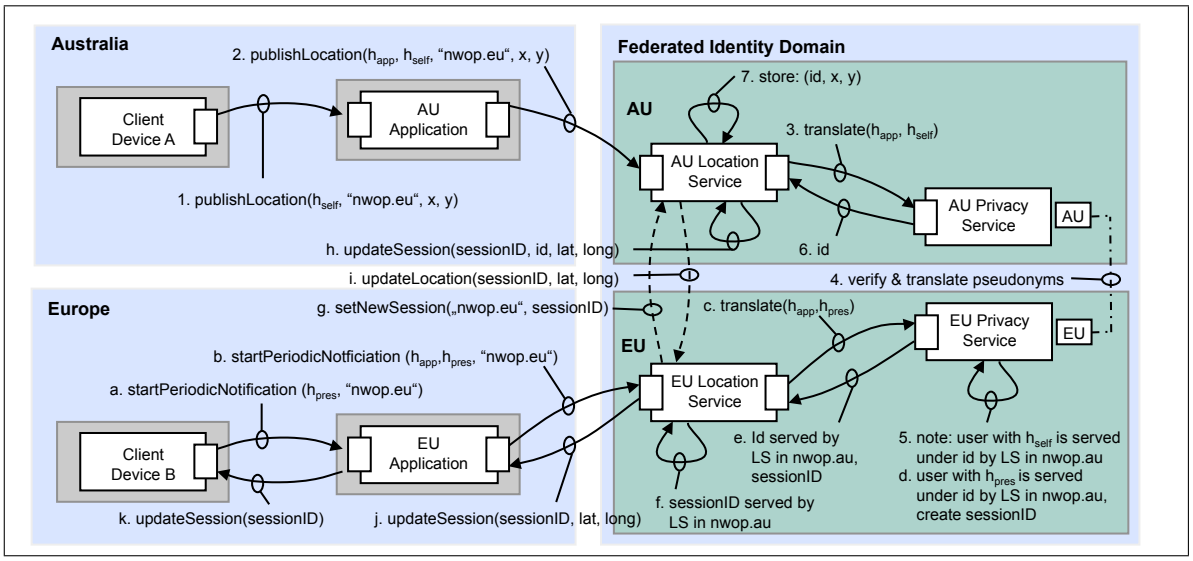

Figure 4.13: Periodic Notification of Location Updates over Different Network Domains [9]

the location is stored by the location server in domain AU, the result is the `id` that denotes user `A` together with the note that the AU location service has recently received `A`'s location information (message e). The EU location service queries the AU location service for the position of user `A`. It sends the `id` in message g. `getLocation(id)` and finally receives `A`'s current location. Messages h. to j. propergate the coordinates of user `A` back to requestor `B`.

Activation of Long-term Processes and Periodic notifications

Finally, we discuss how to exchange and process location data in the federated domain concept by assuming long-term localization processes. First, it requires the establishment of a session context for the applications and the clients. Next, some means are required that allow to convey notifications about changes of locations over the different network domains. Based on the previous explanations about how to exchange location information for a single blocking call like e.g. the `getLocation(.)` request, we now discuss how in the same environment location information is exchanged for the sake of long-term localization processes. The messages 1. to 7. (see figure 4.13 (p. 128)) are initiated by user A in order to update his current location. These messages are quite equal to the messages already shown in figure 4.12 (p. 126). All subsequent messages shown start with message `startPeriodicNotification(.)` that initiates a long-time localization process for user B. Every long-term processes is administered under a certain session identifyer that is created and administered by the respective privacy service. This identifier is propagated to the EU location service (message e) and since this time the AU location service receivces the contact point for location updates from user A the new session is also administered by the AU location service. Messages g. and h. induce the update of the `sessionID` whereas message i. sends the location information to the EU location service. Subsequent messages occur only in case of location changes and are sent in form of notifications. Messages j. and k. deliver the new location information to the application and inform user B about the `sessionID` needed for subsequent administrative purposes.

As concluding remark we want to refer to Adusei et al. [41] which we already mentioned in section 2.2.8 (p. 31) regarding the distinction between three different location request service patterns. The discussion about interoperability between network operators is similar to that of service providers that are not the network operators at the same time. The success of the SMS business case was not possible until SMS functionalities were available on an international scale and thus almost all network operators worldwide. Similarly, the co-operation between internationally operating service providers and network operators will most probably pave the way to location-based services and applications that are worldwide accessible and still chargeable. Another important point that has to be considered here is that in near future different national and international localization technologies will co-exist. The unification of these systems provides other technical as well as legal challenges and will have major impact on the success of future location-based services and their markets.

4.8 Summary

This chapter started with a discussion of the system architecture and its most important components and services which defines the environment. The trust relations between the different providers were explained and how these trust relations can be expressed through different kinds of pseudonyms used throughout this architecture. An explanation of the basic principles of the pseudonym generation scheme and some measurements to assess the performance were conducted. The message interactions for the subscription process and a location request operation was described, equally, the pseudonym chain recovery procedure that is executed in case of errors. The first part of this chapter was finished by assessing the system according to the previously defined classification scheme and based on that possible applications were discussed.

Based on the introductory explanations further functional details were examined. First and foremost the initialization procedure of the so called *self-identifying* pseudonyms. This kind of pseudonyms represent the core authentication token for the initialization of pseudonym chains that are used in conjunction with service calls towards 3^{rd} party application providers. It was further shown that the use of pseudonyms not only protects the user's identity information but further allows for the administration of long-term localization processes that are executed by network operator's and service provider's on behalf of the users. Some aspects of *self-identifying* pseudonyms are comparable with mechanisms as they are applied for the realization of *Off-the-Record Messaging*. These similarities are analyzed in reference to *perfect forward secrecy*, *conficdentiality*, *authentication* and *repudiability*. It is shown that the pseudonym generation scheme not only contributes to the requirement that pseudonyms shall change as often as possible. By comparison with the *Off-the-Record Messaging* scheme it turns out that this scheme also fulfills further requirements that are tightly bound to the requirements of *perfect forward secrecy* (see section 3.2 (p.79)).

The last part is dedicated to the exchange of location information across different network operator's domains. The evolution from formerly separate mobile networks to all-ip based networks also raises the demand for solutions that allow data exchange across different domains. As many aspects of this complex issue are still not solved properly we provide an example that demonstrates the combination of the pseudonym generation scheme with a

network operator specific identity domain. This allows for the the exchange of location information with privacy protection even across different network operator's domain. Given that network operators may offer location information to globally available 3^{rd} party application providers of different domains by still being in control of their customer's privacy sensitive data.

Articles

The following articles contributed to this section:

2. Oliver Jorns, Sandford Bessler, Rudolf Pailer: Verfahren zum Umwandeln von Target-Ortsinfor-mation in Mehrwertinformation Östereichisches Patentamt, Patent No. Austria: Patent Nr. A 363/2004, Submission Date: 1.11.2004

5. Oliver Jorns, Oliver Jung, Gerald Quirchmayr: Transaction Pseudonyms in Mobile Environments, In: *Journal in Computer Virology*, Springer Paris, 2007

22. Oliver Jorns, Sandford Bessler: PRIVES: A privacy enhanced location based scheme, In *Workshop Proceedings of* 6^{th} *International Conference on Human Computer Interaction with Mobile Devices and Services*, Glasgow, September 13 - 16, 2004

23. Oliver Jorns, Sandford Bessler and Rudolf Pailer: An efficient mechanism to ensure location privacy in telecom service applications, In *Proceedings of International Conference on Network Control and Engineering*, Palma de Mallorca, Spain, November 3 - 5, 2004

17. Oliver Jorns, Gerald Quirchmayr, Oliver Jung. A Privacy Enhancing Mechanism based on Pseudonyms for Identity Protection in Location-Based Services. *Australasian Information Security Workshop (Privacy Enhancing Technologies)* AISW-PET2007 *at the Australasian Computer Science Conference in Ballerat*, Victoria, 30 January - 2 February 2007

Article 2 is the patent of the proposed system architecture and the pseudonym generation scheme. It describes a solution that allows to provide added value by inclusion of location information with privacy protection.

Article 5 discusses in detail the pseudonym initialization and user subscription process. By dint of explanations regarding the basic service operations this article also provides a general overview of the whole system and represents a basis for the development of dedicated location-based applications that make use of pseudonyms for privacy protection.

Articles 22 and 23 introduce the proposed system architecture and the basic pseudonym generation scheme. Both articles represent the scientific composition with regard to contents of the submitted patent (Article 2) at this time. The described prototype implementation includes a J2ME client application operated on a HP Compaq 5500 device. The server-side implementation is based on Servlets which may receive only

single `getLocation(.)` requests from the mobile clients. It accesses a dedicated network operator's interface which allows for *cell-based* localizations. The basic functionality of this application was incorporated into the later developed tracking platform.

Article 17 addresses the issue of location-based services for users who roam in different networks or access services that are located or associated to geographical regions that are not under service of the respective home network operator. In such cases, the distribution and the exchange of privacy sensitive data including location information is still difficult in case of cross-domain accesses and even not solved. As a result, the deployment of network operator's services and applications that are available for roaming users is still impossible or at least in its infancy.

Based on the dedicated system architecture this paper extends the use of the proposed pseudonym generation scheme by introducing an identity domain which encloses two or several network operator's domains.

This additional identity domain not only allows for the exchange of pseudonyms across different network operator's domains and the subsequent identification thereof but also allows for the use of service providers that are assigned to different network operators than the user's one. Hence, the introduction of an identity domain between network operators reduces the contractual relationships between network operators and service providers and at the same time multiplies the number of available service providers for the users.

Chapter 5

Implementation Aspects

In the previous sections so far we have presented a solely implementation independent and conceptional view of the proposed system. This includes an overview of the system and its components and also the communication and a description of the interactions between the different components. We continue with a discussion on the most challenging implementation aspects of the location service. This includes the possibility to access and process location information that is received through cell-based localization. Another way to provide the system with location information is discussed in section 4.4.6 (p. 117) and section 4.7 (p. 125) and covers the exchange of location information across different domains. The possibility to allow users to publish their current location represents not only an important feature but further raises interesting questions with regarding optimizing location updates. In order to be able to simulate user motion, we prerecorded location tracks. This allows us to simulate movements of many users at once in a play-back simulation and thus to reconstruct realistic scenarios which is not possible in case of simulations based on random walk.

5.1 Location Service performing Cell-based Localization

In this section we discuss one particular aspect of the location service, that is the ability to retrieve and process location information of users from the network on behalf of users as part of a tracking sessions. One way to determine the current position of users is by using the network based localization that is also called cell-based localization. This represents a prominent and relatively easy way to determine the location of mobile users since it requires network operator to basically provide an interface that allows access the location server. This can be achieved with relatively less technical effort. For the realization of the tracking platform such an interface which provides access to the network operator's location service was offered by a network operator. The location server behind represents one of the core technologies of this platform. For a detailed discussion about the various other possible localization technologies we refer to section 2.2.5 (p. 19). For the case of the implemented location service we assume that the location service is part of the network operators domain, that is, it is located within the trusted domain. It is also conceivable to locate this service outside the trusted domain. In this case additional means for the protection of identities have to be provided.

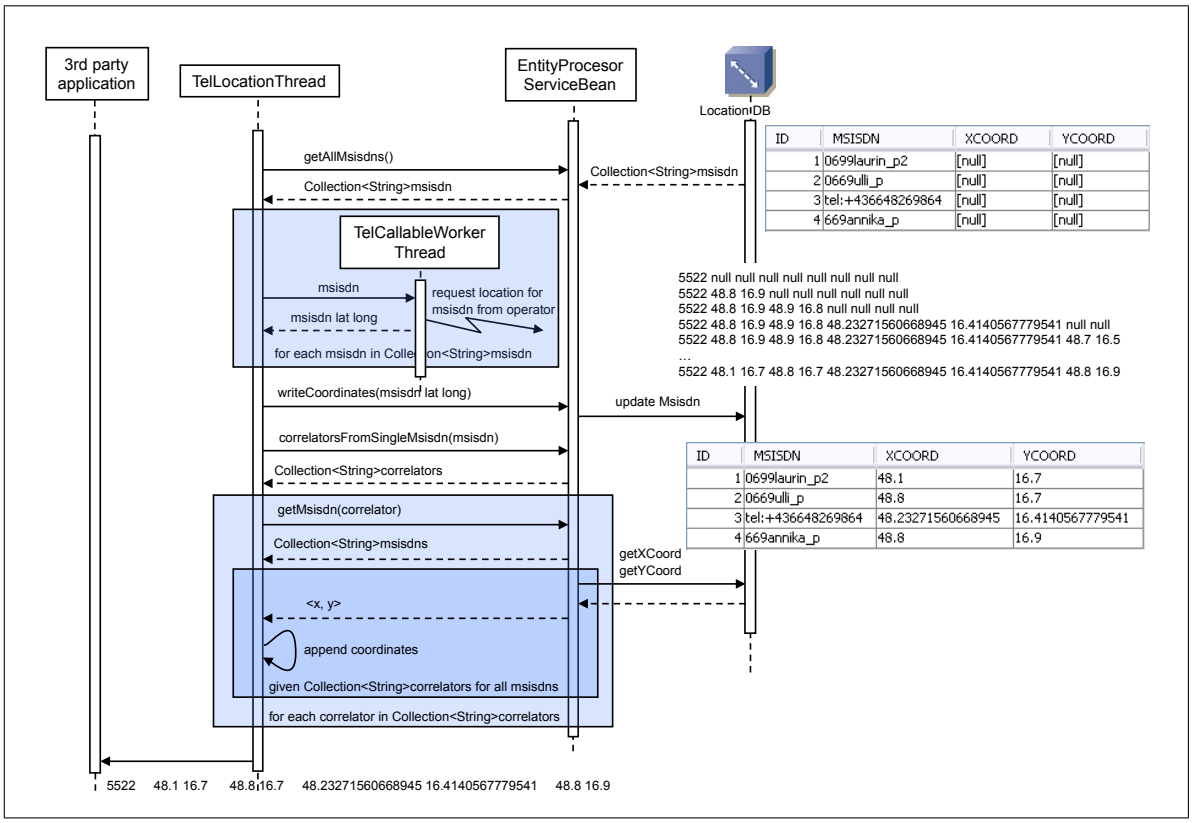

Figure 5.1: Detection, Adaption and Notification of Location Changes

Figure 5.1 shows on the left side the application that receives location information from the network operator and on the right side three implemented entities that are all together part of the location service. There is one thing that has to be noted here. The described entities that are part of the location service and have to be distinguished from the actual dedicated location server that is part of the network. This server is only accessible though interfaces that are under the control of the network operator. Our implementation of the location service may access the location server through a web service interface. The communication line is additionally secured and protected by cryptographic means such as SSL. In order to be able to receive the current location of a particular device, it is stringent that the MSISDN is activated by the network operator. This is necessary because of the legal regulations which prohibit the transmission and use of location information outside the network operator's domain.

In order to receive the location information, each location request contains as argument the respective MSISDN. The actual position of the device as well as the current date and time information for each MSISDN represents the basic function that is used by the location service to manage tracking functionality. Therefore, the `TelLocationThread` process continuously queries the location database for all users that are currently tracked. The request `getAllMsisdns()` returns the MSISDNs of all those users. The database is accessed via a dedicated bean, that is the `EntityProcessorServiceBean`. Next, for each received MSISDN a subprocess called `TelCallableWorkerThread` is spawned that actually queries for the location

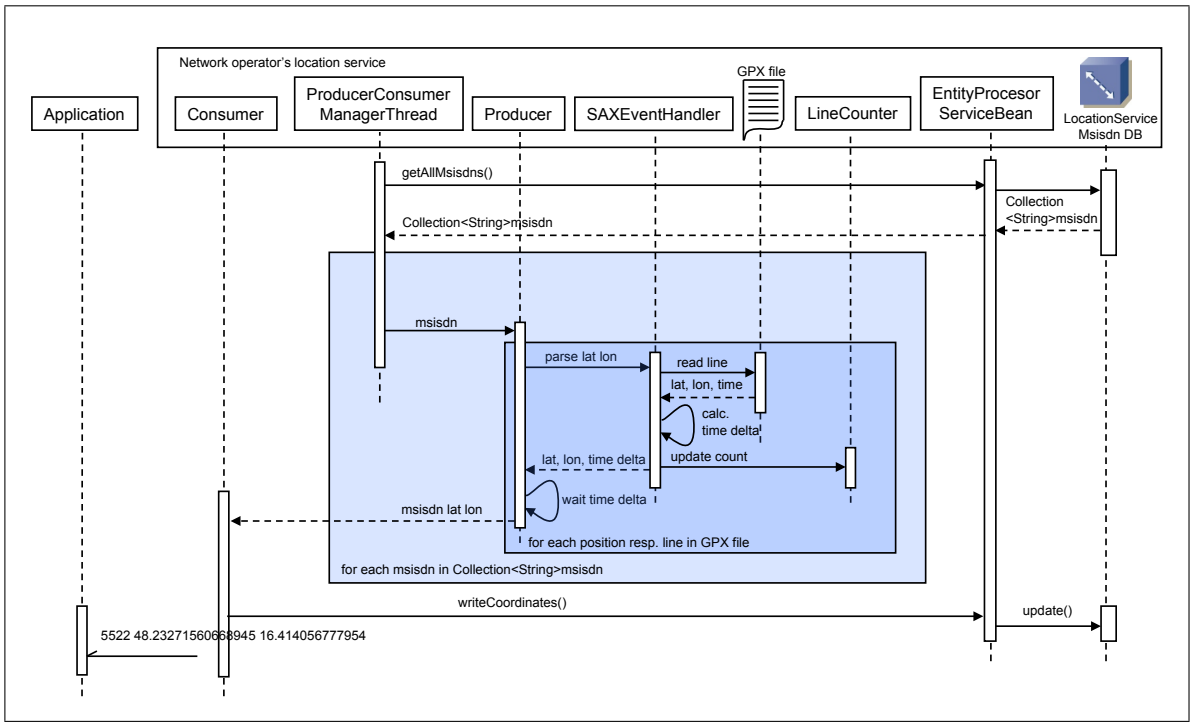

Figure 5.2: Location Service Processing Location Information Stored in GPX Files

of that MSISDN from the network operator's location server. Figure 5.1 shows this processes as an arrow that is denoted with *request location for msisdn from operator*. Finally, the location information is written into the location database. Since each user may be administered concurrently under several sessions and each session may in turn administer several users, *TelLocationThread* first queries for any session that administers the particular user whose location has changed (message `correlatorsFromSingleMsisdn(msisdn)`). Then, for each correlator that is contained in the received collection of correlators, *TelLocationThread* iteratively queries for the respective msisdns of each correlator and retrieves the current location from the location database. The generated message contains the correlator and the locations of each msisdn that is administered under that correlator. In figure 5.1 this message is `5522 48.1 16.7 48.8 16.7 48.23271560668945 16.4140567779541 48.8 16.9`. The first value is the correlator which is followed by the coordinate pairs of the users who are administered under this session.

Figure 5.1 also shows how each of the four coordinate pairs of session `5522` are gradually adapted. This stepwise adaption of the location information arises from the iterative queries for each msisdn. The depicted example shows that four such iterative cycles were needed till all coordinate pairs were allocated with positions.

5.2 Location Service processing GPS Locations read from GPX files

In section 4.4.6 (p. 117) we discussed the availability of localization technologies for mobile devices like GPS that enables them to determine their current position on their own and thus send location updates to the tracking platform.

In this respect, this section discusses an extension of the system that aims at simulating even a huge number of users that are tracked simultaneously. We achieve this by processing recorded GPS tracks which provides a number of advantages. One is that the use of stored GPS tracks may alleviate the development process of location-based services. During the development process there may be only a limited number of users that are equipped with mobile devices that can be located constantly. In case if special tracks or movement scenarios are required, live-tracking is definitely not applicable, since developers have to reckon that certain users are not in the desired position or may not move along the desired way. Another advantage that comes along with the use of recorded GPS tracks is that with this it is possible to investigate different performance issues of the system. This includes not only the location service but also the application's logic.

Figure 5.2 shows the message diagram that makes use of the classic *Procuder-Consumer* relationship [174] (p. 290, 305). Here, the main daemon process that is called *Producer-ConsumerManagerThread* that administers a number of multithreaded *Procucer-Consumer* threads. As the number of *Consumer*s is arbitrary and can be regulated by the operator, the number of active *Producer*s mainly depends on the number of MSISDNs that are received from the location database. Each *Procuder*s assigned to a certain file that encodes location data according to the GPS Exchange Format (GPX)[1]. The following XML snipplet of an GPX file shows different sections including tracks and track segments which contain track points and coordinates. A track point contains the elevation information and a time stamp when the track point was recorded.

```
<trkseg>
  <trkpt lon="16.156835" lat="48.299493">
    <ele>168.000</ele>
    <time>2007-08-13T16:21:11Z</time></trkpt>
  <trkpt lon="16.156400" lat="48.298952">
    <ele>168.700</ele>
    <time>2007-08-13T16:21:28Z</time></trkpt>
  <trkpt lon="16.156138" lat="48.298808">
    <ele>168.900</ele>
    <time>2007-08-13T16:21:34Z</time></trkpt>
</trkseg>
```

The *Producer* plays-back the recorded track. Therefore it first reads the coordinates together with the associated time stamp of the first track point and, in addition to that, the time stamp of the successive track point. The coordinate pair of the first track point is passed to the consumer thread. The producer computes the time difference of consecutive track points (*calc. time delta*) and uses this value to set itself to an idle state. When the producer wakes up, it continues to read the coordinates and time stamp of the second track point. The

[1]The GPS Exchange Format GPX is an open exchange location format. It is based on XML and was developed by TopoGraphics, http://www.topografix.com/gpx.asp (last viewed 6. Jul. 2009)

respective line number is stored in a Singleton class called *LineCounter* and is adapted in such a way that it can also be used in a multy-threaded environment as it is typically encountered in servlet containers with multiple class loader [175]. The time difference of the n^{th} and $n-1^{st}$ line, the respectively the two consecutive track points, is used to calculate the next idle time. This continues till the last track point is reached.

As the *Consumer* receives the coordinate pair for an MSISDN (message `msisdn lat long`) it updates the location database (`writeCoordinates()`) and forwards the session identifier together with the coordinate pair(s) as part of a message driven bean to the application (message: `5522 48.23271560668945 16.414056777954`).

5.3 Motion Simulator Module

In this section we discuss the design of a motion simulator module which makes use of the pre-recorded GPX tracks. Similar to the described development tools introduced by Aitenbichler [176] that aim to support developing distributed, loosely-coupled context-aware applications, this module is a first step towards assisting developers in the development of location-based applications. At this stage it primarily allows for the visualization of the actual position of each tracked user. This reflects the basic idea for the realization of the management interface that makes use of the motion simulator and provides developers means and a tool to evaluate and test the behaviour of future applications without the burden to implement the whole back-end system.

As discussed in the previous section, the actual content of the location services database is the starting basis of operation for the *TestEventPullSources* module. This module is part of the pushlet framework [2] which allows to send events asynchronously to a browser. Therefore the pushlet framework first registers GET requests that are originating from the bowser but keeps the connection open instead of closing it. Hence, the browser has to wait until it receives the command to close the connection to the server. Instead of sending this command, the browser is provided with data that is subsequently processed and shown on the website.

The process `TestEventPullSources` shown in figure 5.3 first requests all MSISDNs and their coordinates from the location database. The received collection of all the user's identifiers is compared to the cached version in the hashtable. This hashtable represents some kind of mirrored location database and is synchronized each time a list of identifiers was received from the location service's database. In the most simple case synchronizations are only processed when `TestEventPullSources` has received the actual list of MSISDNs. The reason why all MSISDNs that are currently stored in the localization database are also cached in the hashtable is mainly to minimize the communication to the browser.

Every time `TestEventPullSources` receives a list of MSISDNs from the location service's database, the synchronization process stores all those MSISDNs in the hashtable that are not already stored there and generates a JSON [177] object. Figure 5.3 shows an example of such generated JSON event objects. It represents an array that is denoted as `msisdn`. Each element of the array contains the user's name, the filename (in case of cell-based localization the filename is replaced by the actual MSISND of the particular user), the coordinates and the activity. Once the JSON object is set up it is transferred to the bowser which then

[2] Pushlets: http://www.pushlets.com/ (last viewed 6. Jul. 2009)

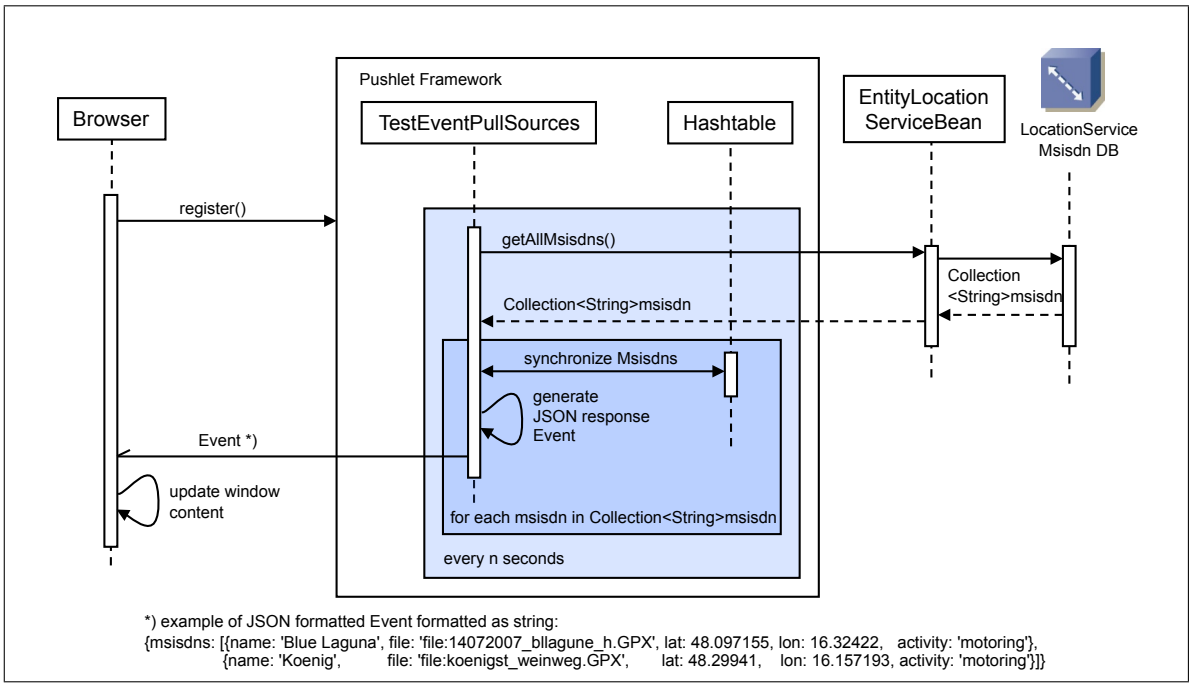

Figure 5.3: Instant Event Notification on Location Changes

processes the contained data. In case the hashtable contains more objects than received from the location service's database this means that one or several users were taken of from further localizations. By removing the respective objects from the hashtable the cache is updated and reflects the actual state of the localization database status.

In addition to equalizing the number of objects in the cache with the number of objects received and subsequently generating JSON objects from each retrieved object that was not found in the cache, next the location information of all received objects that are also in the hashtable are compared. Now, the JSON object is further extended by those objects that contain different locations. This means, the JSON object contains either objects that were not found in the cache, contained different locations or both. Finally, all object that are in the hashtable and provide different locations have to be updated. The example in figure 5.3 shows that the position of two objects namely `Blue Laguna` and `Koenig` have changed their position. The event is formatted as JSON string and can be processed by the browser.

It is clear, that for the operation of the motion simulator the protection of the user's privacy is rather secondary. The used underlying technologies are indeed also based on pseudonyms. But, the collection of modules that represents the motion simulator module has access to the user's information. This is realized by allowing direct access to the same modules and makes in this case even sense as the purpose of this module is basically to support the development process of location-based service and applications.

5.4 User Management

Another important aspect is how to map and store existing user relations. The initialization procedure of pseudonyms is described in detail in sections 4.4.2 (p. 113) for self-identifying pseudonyms and 4.4.3 (p. 116) for pseudonym chains that refer to relations of individuals.

After these initialization procedures the resulting relations, pseudonyms and other identifying credentials have to be stored. This requires access to legacy databases that store these credentials. As each implementation depends on the respective existing infrastructure and available technology, in the following we provide a rather generic and implementation independent view on how this information can be stored. For this generic view we encode all information in XML files which are explained in the following.

The following code snippets show different sections of this XML file. It starts with the obligatory header and continues with the definition of the root `<watcher_presentity_db>` which contains as attribute the session identifier `sessionId`. Next, the definition of the user list that is denoted by the tags `<userList> </userList>`. Each user in the user list is a `watcher` that is associated with some activity such as `biking, racing`. A watcher also has an identifier like the MSISDN. As shown in the code snippet below, the MSISDN is in this case replaced by a filename, e.g. `file:bikingracing.GPX`. Users may watch other users and also be watched by users. Thus, watched users are listed in the watcher's `<presentityList></presentityList>`. Below, the example shows a watcher that has only one presentity that is called `Hannes`. If the watcher requests any information about this presentity, she must provide the right pseudonym which is referred by the argument `pseudonym`. In addition to the `password` and the `activity` each presentitie's section also provides an attribute that denotes the identity. As for network-based localizations our system requires to provide the MSISDN we also named the identifying user attribute `MSISDN`. As in this particular case the `presentity` attribute is associated with a pre-recorded GPX file, the `MSISDN` attribute has assigned the filename `file:biking racing/Hannes.GPX` as identifier.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<watcher_presentity_db sessionId="1">
  <userList>
    <watcher name="biking, racing" ...>
      <presentityList>
        <presentity name="Hannes"
            password="phannes"
            pseudonym="c26834fb629f36ngfg7n2d6fju76564c7m9ld531"
            activity="biking, racing"
            msisdn="file:biking racing/Hannes.GPX"/>
      </presentityList>
    </watcher>
    ...
```

The following code snippet shows another watcher - presentity relation. Here the attribute `presentity` refers to the a real MSISDN. The scheme `tel:` in`msisdn="tel:+ xxxxxxxxxxx2"` indicates that the location information is not retrieved from a file but from the network. The code snippet also shows that one or more presentities can be grouped together in a

<presentityList> that is assigned to one watcher. A watcher must not be a dedicated user. Instead of that it can be interpreted rather as a category of a motion pattern or a topic. The current implementation supports the following categories *motoring*, *CellId file* or *CellId real*. Any kind of additional category is conceivable.

```
    <watcher name="CellId real" ...>
      <presentityList>
        <presentity name="Ulli"
            password="pulli"
            pseudonym="26c4617595dc8fc9ff86c94cc21569be658b1234"
            activity="cellid"
            msisdn="tel:+ xxxxxxxxxxx2"/>
      </presentityList>
    </watcher>
```

The last code snippet below shows the case of a watcher that is at the same time the presentity. This variant of pseudonyms we call self-identifying pseudonyms (see section 4.4.2 (p. 113)). Such pseudonyms can be used for applications like the transport ticket application which is discussed indetail in section 6 (p. 149) or any other position-aware or self-referencing location-based application (see section 2.2.6 (p. 24)).

```
    <watcher name="SelfAnnika" ...>
      <presentityList>
        <presentity name="Annika"
            password="pAnnika"
            pseudonym="f82b9f834br3gbd1710b1824aaa05f265eff2156"
            activity="motoring"
            msisdn="file:Annika.GPX"/>
      </presentityList>
    </watcher>
  </userList>
</watcher_presentity_db>
```

5.5 Management Interface

The management interface allows to easily administer different localization sessions and thus the simulation of several mobile devices. As depicted in figure 5.4, the grey table on the left side shows all details about all active sessions such as the session identifier, the name of the watcher (e.g. last session nr. `50` with simulation watcher name `CellId real`) and the tracked users who are listed under column *buddies* (e.g. `Ulli` and `Sani`) and in the last column the actual position of each buddy. New sessions are started by first selecting a user from the topmost selection box. For each selected user a list of the respective buddies is shown. For each selection of one or more buddies a new session can be established by pushing the `start new session` button. Sessions can also be stopped again. By pressing the respective stop button `(->)` in the first column. On the right side the icons indicate the actual position

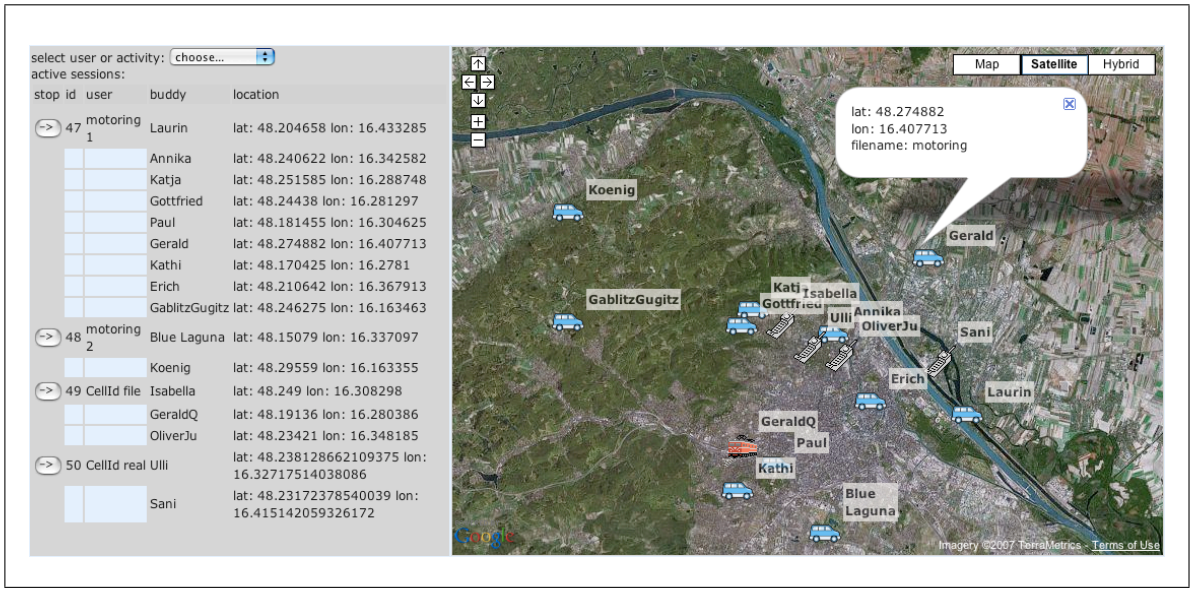

Figure 5.4: Management Interface with Integration of Google Maps [10]

of each tracked user. For that we used the API from Google maps[3] which allows to depict the position of each user that is encoded in received JSON object. Furthermore, the type of movement of each user is distinguished and shown with the corresponding icon. The picture shows some possible types such as cars, trains and mobile phones. Whereas the cars represent recorded GPS tracks, the train and the mobile phone icons are recorded cell-id movements. If an icon is clicked, the speech bubble shows the actual location and the filename of the recorded track. All this information is passed along with the JSON object. For example, the filename is encoded as `activity='motoring'`. As each received JSON object contains only those objects whose location has actually changed, this kind of notification represents the least possible communication overhead.

5.6 The Managmement Module

The implementation of the management module primarily aims at supporting the development and test phase of location-based applications in general as well as their particular modules, operations and additional functions. The current implementation of the platform allows developers of location based applications to actively control sessions and select certain tracks to simulate motion scenarios. Given that developers may concentrate on the important aspects of their applications. The platform provides all the means that are necessary for the realization of location updates and means of notification which significantly reduces the complexity developers face during the development of location-based applications. In this respect, we can summarize the following requirements:

[3]Google Maps http://maps.google.com (last viewed 9. Jul. 2009)

facilitate the development process of location-based applications this allows developers to implement only the most important moduls first. This includes computational intensive modules that process positions of several users, the calculation of routes and the inclusion of additional services that operate on available position data to name only a few.

provision of a simple and transparent privacy mechanism that can be deployed to legacy mobile devices with even low processing power and memory constraints. Another advantage is that the pseudonym generation scheme does not require any additional infrastructural measures and can be used even during the development and testing phase.

the management interface allows for rapid testing of any kind of applications including both, real and simulated user motions. With prerecorded motion paths it is thus possible to also reproduce motions. With this, certain constellations or behavior can be reproduced. Based on such dedicated scenarios it is also possible to investigate slight deviations and combinations of motion tracks which result in *what if* scenarios.

5.6.1 Possible Future Development on the Management Module

The implementation of the management module as it is shown in figure 5.4 (p. 141) allows for the administration of tracking sessions. Tracks are either created artificially (random walk) or read from a database which stores recorded tracks. In the latter case software tests may require much preparatory work which includes the collection, preparation and combination of different test tracks before they can be integrated into the system. If real user motions are required, the matter becomes even more complex.

The current implementation state provides only location changes that detected by the location system. Similarly, location changes are only recognized by the location service and published to the management module. Except for pre-recorded tracks that are played back, or real user motions which are unfeasible in most cases there is no other way to generate location changes and events. This single track line of information may present a bottleneck since it does not allow the tester to intervene active processes when needed.

One possible extension of the system would be to allow the developers to use the management module not only to start and stop sessions with predefined tracks but also to use this to actively publish location information to the location service. This can be accomplished by allowing developers to e.g. move icons that represent virtual users or objects. Each time an icon is dropped at another position, a location-update event is generated whereupon the location information is then propagated to the location service. This procedure is correspondent to location updates initiated by real user's motions or played-back tracks. The same capability is also provided by the *WorldView* tool proposed by E. Aitenbichler [176]. Furthermore, this allows also to simulate indoor location updates which is beneficial in many cases.

At the time of writing this thesis, the system processes recorded tracks that are stored by GPX files (see section 5.2 (p. 136)). Each such file represents one particular moving object, that is e.g. a car, a mobile device or someone taking a walk. The more users are tracked, the more files have to be parsed. The longer each track is, the more lines have to be read till the last remembered line, that is the respective next track point, is reached. As each track may contain hundreds or thousands of track-points it is obvious that with many tracks

processed in parallel the platform cannot guarantee high-performance. Thus, it is reasonable to store all tracks in a database which can be accessed with a single request. This further requires conversion tools that allow to store the track-points that are contained in the GPX in the database. In addition to the gained performance, the use of databases further allows for the generation of random walk tracks. To avoid that tracks are generated on-the-fly without orientation, instead each track can be generated between two randomly selected points with a random speed. It is also conceivable to allow to select departure and destination regions to limit the dimension and number of tracks. Finally, the inclusion of real-time information such as traffic or weather conditions may be a viable source for the creation of virtually realistic scenarios.

5.7 Access and Update Strategies to Remote Resources

Modern telecommunication networks and systems rely on dynamically changing information. Equally, location-based services rely on highly dynamically changing information, that is basically location information. The design and implementation of each such highly dependable system does not only affect technical but also organizational matters. In the following we concentrate on very specific technical aspects of location-based services that is the exchange of location information between the various players. In particular, we emphasis on different possible location update strategies as they can be implemented by the clients. Second, we focus on access strategies that are most relevant but not restricted to the telecommunications services, namely that of the location service. As we will see, all of the presented models and concepts are not strictly bound to one particular entity such as the client or a network service but can also be part of any other entity within the system.

5.7.1 Client Side Update Strategies

In this section we discuss different client side update strategies for location information. On important aspect that has to be considered during the design an implementation of software for mobile clients in general is if the provided solution may be too computational intensive and thus not be applicable by some devices. More generally, the efficiency of such solutions mainly depends on and can be measured by the *access delay* that is caused by the (GPS) sensors. As a result the it is questionable if the location information of the client is *correct* and *accurate* enough. Finally, the update strategy also determines the *network traffic* which, if not properly chosen may result in *network overhead* that in turn may lead to efficiency losses in terms of correctness and accuricy. Even though the evidence of these efficiency factors there are also additional constraints to be considered which mainly rely on the respective application at hand. For the client side we distinguish three different kinds of location update strategies. They are referred to as *(1) constant*, *(2) speed dependent* and *(3) path dependent*.

The Constant Update Rate Strategy is rather simple since it sends location information in fixed time intervals. Due to its many drawbacks opposed to other update strategies this strategy should only be implemented if it is really requested by the application. Otherwise, it should only be used for test purposes or during prototyping. Many GPS

car tracking solutions[4] implement this simple strategy. The reason behind that is that it allows transparent calculation of all transmitted data chunks of each certain time period. This transparency makes calculation of costs easier.

J. Krumm [131] refers to *Dropped Samples* as an additional countermeasure against inference attacks, it is possible to reduce the identification rate of individuals from 85% to 40% just by reducing the GPS sampling interval from only one minute to four minutes.

Software that implements the location updates with fixed update interval produces in any case also redundant location updates and network traffic. To overcome these drawbacks, the inclusion of the speed of objects may constitute an advancement in terms of network utilization by reducing the transmission of location information to a minimum. The location update strategy that also takes the speed of objects into account is subject matter of the next point.

The Speed and Time Constrained Update Strategy takes into account the speed of a moving object and thereupon calculates when the next location update message has to be sent. This scheme is much more flexible than the scheme with constant delays between the location update messages and further allows the adjustment of the precision of location updates according to the covered distance between two consecutive measured points. The scheme sends location update message only when the object has covered a certain predefined distance. The faster objects move, the more location updates occur. To prevent from too many location updates when the objects move very fast, two possible adaption procedures that can be applied. Either the threshold distance or the time interval between each location update message is adjusted to the actual speed of the objects.

Speed and time dependent update schemes require less update messages which in turn utilizes the network better by still providing meaningful and accurate information about the current position of the clients by also reflecting better the actual movement pattern.

This scheme further better complies with the so called *need-to-know principle* which aims to ensure that individuals release only enough information that a service provider needs to know to provide the required service.

Similarly to measuring the speed of objects and based upon that the transmission of position data, the receiver may also complementary and proactively anticipate the respective current position of the user. By calculating the actual approximate speed of the object, receiver may continuously extrapolate the very next positions or even the path of the clients which, quite evidently, may better serve the users requests.

Path dependent update rate This strategy does not exclude any of the strategies discussed before. It can rather be seen as a refinement of the speed and time constrained update strategy with the inclusion of information about a portion of the clients track. Therefore, as the client receives a series of positions it first buffers and then analyses them. As long as the consecutive chain of at least the last three positions form a straight

[4]GPS traking solutions: http://www.pimall.com/nais/tracking.html (last viewed 7. Jul. 2009)

line with only minor deviation the client does not have to transmit any location information at all. As soon as the last received position deviates from the continuous line of the previous two points by a certain angle, the clients sends the last two positions.

As a result, this strategy requires to send only those location information that describe the shape of the route best. Movement patterns of cars driving with reasonable speed on highways utilize this kind of strategy best. However, in case of very slow motions or when objects stand still this strategy does not meet its full potential. Objects that stand still receive only constantly changing and deviating location information from the GPS receiver. Irrespective of the small scale in which these location changes occur, the received positions are interpreted as permanent deviations which causes the client to transmit its current location. Thus, advantageous to include the speed and time constrained update strategy in order to avoid unnecessary location updates when the objects moves slow or stands still.

To conclude the short discussion about possible clients update strategies, the examples clearly show, that various factors such as the speed of the object and the location update interval determine the precision and quality of the location information. Furthermore, not only from the network operators point of view but also from the customers point of view, the network utilization is still of major importance. Although most pricing schemes are meanwhile based on the data volume exchanged rather than on time, heavy usage of applications that do not consider optimized data exchange may flood the network with needless messages and drain faster the mobile devices' battery. But, optimizing services on the client side is certainly not enough. It is at least important to examine carefully those services and applications that generate and process the location information.

5.7.2 Network Services Access Strategies

The following discussion about access strategies is structured according to the presented work of Rasmus et al. [16]. For the in depth discussion on the analytic models of access strategies we refer to their publication. The observations, are strongly related to the functional description of the tracking platform described in section 4 (p. 91). Rasmus et al. distinguish in [16] the following two possible approaches:

Reactive/on-demand requires the requester to actively query for the location information. The underlying system architecture equates the client-server architecture. This approach is conform to services that provide location information on request. The advantage of this approach is that the location information is transmitted to the requester only when it is needed.

Pro-active in contrast to the reactive/on-demand approach, this time receiver of location information do not need to actively query for location changes. Instead of that, location changes are rather submitted by the entity that is simultaneously the source of the location information.

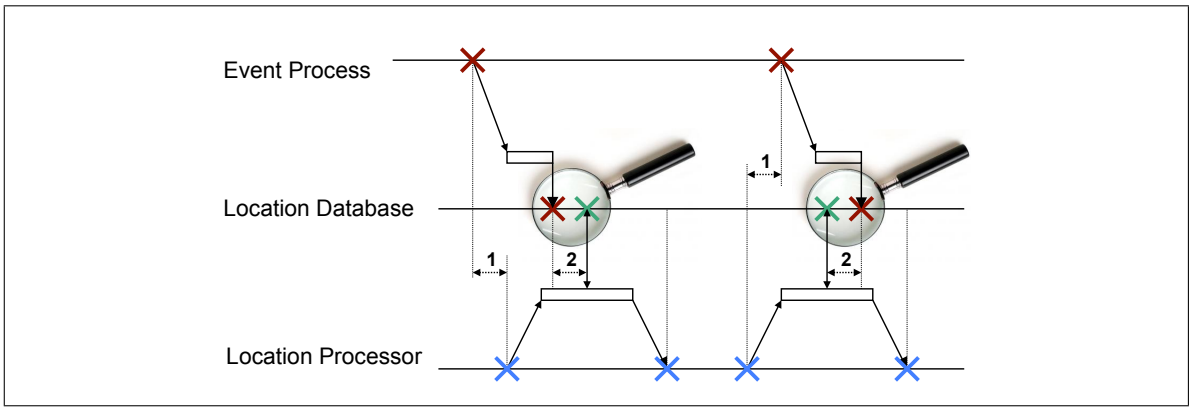

Figure 5.5: LocationEvent Updates and Processor

This approach allows the distinction of two sub-categories.

- *event-driven* which refers to processes that immediately send the location information upon change to the receivers and
- *periodic* which refers to processes that send location updates in constant intervals.

Our platform implements combinations of both approaches. Whereas the clients are informed pro-actively in an event-driven way, the location service queries the location of mobile users reactively. The clear distinction between the different update strategies allows for better estimations on the network traffic and determines which technology to apply. However, each particular strategy may in certain cases also provide some deficiencies that have to be considered carefully from case to case. In case of reactive/on-demand accesses it is clear that the client does not know when the next location update actually occurs. Clients that implement such a strategy may simply guess when there is a location update and justify the update-request period on that. It is clear that simply guessing is the worst strategy in terms of network utilization and consumption of other resources. The advantage of pro-active strategies opposite to the reactive/on-demand one is that in this case the information can be transmitted as it occurs. But, as R. L. Olsen in [16] show, as soon as the location of an entity changes the change can be communicated to the client. Figure 5.5 shows a combination of the discussed *reactive/on-demand* and *event-driven* processes. The *reactive/on-demand* process is represented in the figure by the Location Processor that is the client that requests for the location of another user. The Event Process represents users who change and convey their location to the location servers' database. In this case the Location Database is at the same time the requester of the location information.

Two possible significant request-event constellations are possible. One assumes that the location update event occurs before the location processor requests a location update and vice versa. Both cases are depicted in figure 5.5. On the left side the event occurs before the request. It is received and stored by the location database right before the requester. The example on the right side represents the case when the event occurs after the location processor sends the request. Then, the request is processed before the location update event is received which makes the received location information obsolete.

5.8 Summary

The implementation of the tracking platform was basically a proof-of-concept implementation of the pseudonym generation scheme. The first part of the implementation description refers to a module that allows for network-based localizations. This represents the basic localization method of the tracking platform. The second module allows for the processing of pre-recorded tracks that are stored in GPX files. With it, both, recorded network-based tracks as well as GPS-based tracks can be played-back via the tracking platform to simulate user's motion. In order to ease the management of long-term localization processes a web-based management module was developed. With it, the position of moving objects is visualized to be traced.

Apart from the realization of concurrent localizations processes and the management thereof, it turned out that the platform is further qualified as basis for rapid development of any kind of location-based service and application development. It allows system and application developers to concentrate on particular aspects only or test specific functionalities of their system without the need to set up the whole infrastructure before.

Another important outcome of the proof-of-concept implementation was the identification of different access and update strategies which may have strong influence on the design of systems that in general, rely on remote resources. One such example is the location service. We differentiated between the client side strategy and identified *constant* then*speed and time constrained* and finally *path dependent* strategies. There are certainly many different further possible schemes that allow clients to convey location information to the location service. With these three examples we could illustrate that the design of location-based services mainly depends on different, partly contradictory conditions such as network utilization, accuracy and finally scalability and that these factors may vary to a great extend from the chosen client's location update strategy. In the same course we also highlighted network access strategies where we distinguished between *Reactive/on-demand* and *Pro-active* ones. The latter case can further be distinguished in *event-driven* and *periodic* ones. Finally, the presented examples reveals the problem of different request-event constellations which have to be considered in case of receiving asynchronous update and notification messages.

Articles

The following articles contributed to this section:

12. Oliver Jorns, Oliver Jung, Gerald Quirchmayr. A Platform for the Development of Location-Based Mobile Applications with Privacy Protection, The 3^{rd} *International Conference on COMmunication System softWAre and MiddlewaRE* (COMSWARE 2008), Bangalore, India, January 6-10, 2008

Article 12 starts with a description of the proposed system architecture and the available functions of the implemented tracking platform as well as the integrated pseudonym generation scheme for the protection of privacy sensitive data. In general the paper aims at easing the development process of new location-based applications. Since the development applications which access, receive and process user's location information requires a dedicated underlying infrastructure which may consist of complex components that are often not available or difficult to provide, the discussed platform provides

a solution for both, developers and analysts in equal measure. Whereas developers use the platform as a starting basis for the development of dedicated modules or even whole applications, the latter one may conduct analysis about the implications of certain constellations without the need to build the whole system. Thus, the proposed platform leverages the conceptual analysis and eases the development process of dedicated modules.

Chapter 6

A Transport Ticket Demonstrator

As already indicated in the previous sections, the combination of the presented service architecture and the proposed pseudonym generation scheme allows for the development of various different applications that make use of location information. In the following we show how even existing implementations such as ticket applications may be extended to allow users to enable processing of their own location information which represents a significantly increasing added value. The implementation of this demonstrator does not implement the pseudonym and location information processing capabilities yet. At the time of writing this dissertation this is considered rather on a conceptual level.

Compared to the existing paper-based transportation ticket, the digital version offers advanced functionality. One feature that can be realized by the use of electronic transport tickets is the ability to allow users to exchange their tickets with others. Therefore the owner of a ticket receives a unique key which is transmitted e.g. via phone call to the receiver of the ticket. Upon receipt, the receiver may acquire control of the ticket for a certain time span. For example, a ticket with a validity period of a month can be transferred to another user for 1.5 hours. After the expiration, the ticket is automatically returned to the ticket owner.

This is only one out of many possible features which adds value to existing solutions and make the use of digital tickets more attractive. With the integration of location information the scope of possibilities is further extended. In the following we demonstrate our solution of a transportation ticket application which can be implemented on top of our service architecture and thus integrate the user's location information.

6.1 The Transport Ticket Process

The ticket process reflects the whole ticket life-cycle of a transportation ticket, beginning with the user's registration till the end of the validity of the ticket. Each step of this life-cycle is described in the following. Additionally, this illustrates the user's interactions and explains some details about specific characteristics of transport tickets that are important for the implementation. Finally, on a rather technical level we describe some of the messages that are exchanged between the users, the transportation ticket provider and the network operator. This description also includes the pseudonym scheme which is actually not implemented in this prototype and must thus be seen as an conceptual analysis.

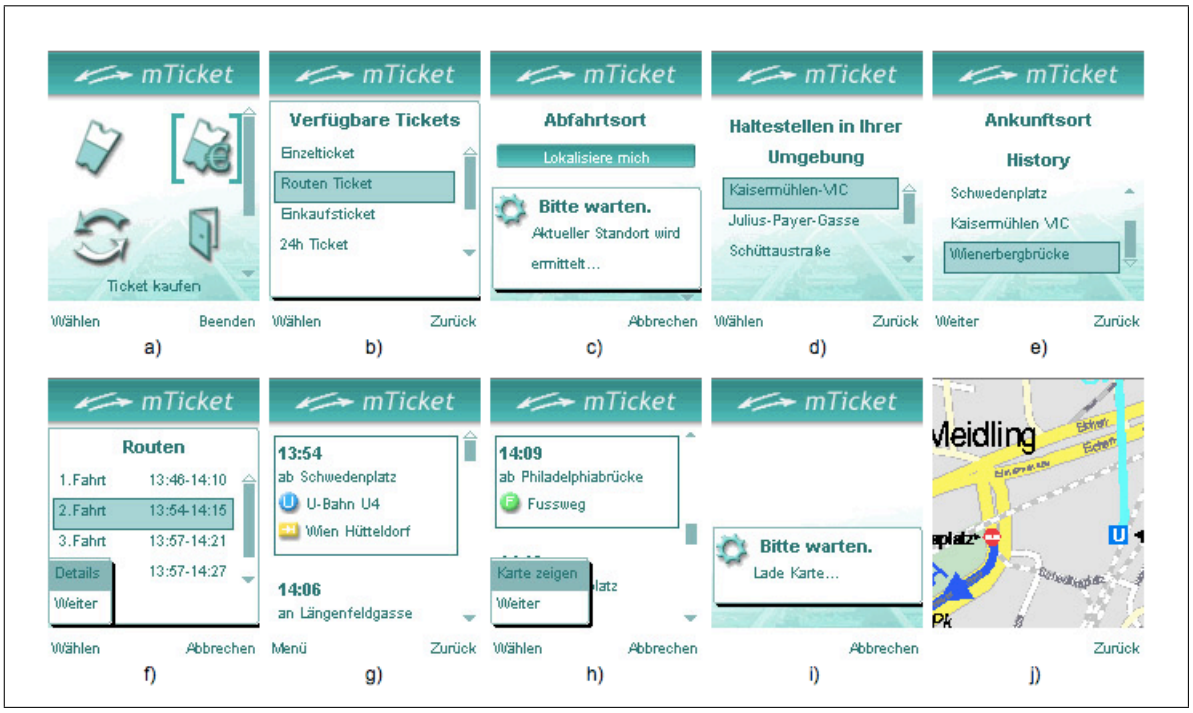

Figure 6.1: Ticket Configuration [11]

6.1.1 Ticket provisioning

Before one can buy tickets she has to register at the ticket portal page. This page provides the user with a detailed description of the ticketing service, its features and payment details and as well as a step-by-step guideline how to register to the service. The user is first asked to enter personal information such as the desired username, password and the telephone number of the mobile phone from which the tickets will be requested. As the user account is created at the ticketing application server she is next redirected to the payment portal of the payment provider where she is asked for the preferred payment method. The connection is secured by means of https. Finally, the payment-provider creates a payment-account for that user and charges 10 Euro. Users may access and charge their payment account at any time.

Download Terminal Application

After registration, the one can either navigate with the browser to the download-portal on the web page of the application service provider (Figure 6) to first download the mobile application to the personal computer. By doing so, the software has to be installing by the user herself on the mobile terminal. It is also possible to navigate the mobile terminals browser to a dedicated WAP-portal that allows to download and install the terminal application directly onto the mobile phone.

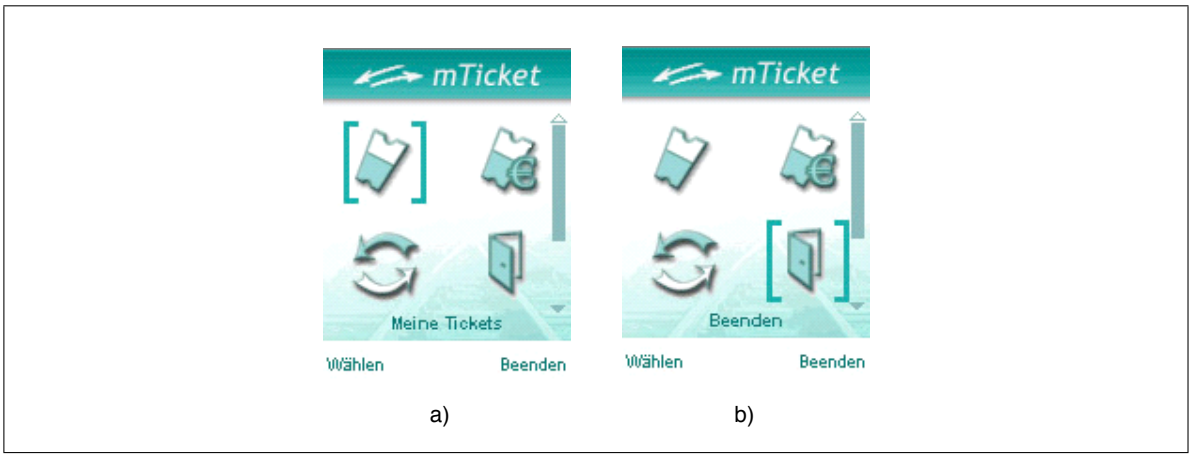

Figure 6.2: The Mobile Application's Main Menu

6.1.2 Invoking the Mobile Application

As the software is installed on the mobile, users may request, buy, view and transfer tickets. Furthermore, they may check their own payment account and change personal settings. In this section we describe in detail each of these operations. When the user invokes the ticketing application, the main menu shown in figure 6.2 provides icons, each representing a certain ticket operation. The first operation that is described in the following is that of requesting new tickets. The application provides three different kinds of tickets:

- *Transport Ticket*: this kind of ticket is valid for a maximum of 1.5 hours and for one route. It provides no additional functions such the inclusion of location information or transferability as it is provided by route or time tickets. In the strict sense, this kind of ticket simply represents the electronic version of the classic paper based version. It is particularly used by users who occasionally use public transport.

- *Route Ticket*: In this case the user is asked to first configure the ticket, that is, she is asked to provide the departure and arrival stations. The departure station is either entered manually by the user. Another possible way that is even more convenient for the users is to first determine the actual position by means of localization that is undertaken by the network operator. The location information is then used to retrieve the nearby stations. By being able to locate users this functionality can also be extended to a tracking function. Thus, if users agree with continuous localizations this enables users to receive additional information according to their current position. Thus, tickets that may also integrate localization technologies may provide the ticket owner with additional functions that are even far beyond the classic perception of transport tickets. Such tickets may provide users with informative messages and notifications about certain evens such as delays or propose new connections. It is also conceivable that the price of route tickets depends on the respective route the user chose.

Figure 6.3: User buys a Single Transportation Ticket

- *Time Ticket*: this kind of ticket is limited in time and referred to as shopping ticket , 24h ticket, 72h ticket, week ticket or month ticket. Additionally, monthly tickets are also *transferrable*. This means that the owner who paid for the ticket may hand it over for a certain period of time. This is done by exchanging a certain code between the ticket owner and the receptor. The code may be exchanged orally or any other available means of communication.

6.1.3 Configuration of a Single Ticket

Users are not limited to buy only one transport ticket during one session. Each request and thus each session allows users to order even more than only one single ticket at once. Figure 6.3 shows in detail an example flow of this process. It starts with the first screen (a) where in this case the user decides to select a single ticket. The next screen allows to decide how many tickets shall be ordered at once. In this example only a single ticket is requested. If the user wants the ticket to be activated immediately as it is bought, the ticket will be transferred to a dedicated folder that stores all tickets that are activated. Otherwise, as in the case depicted in (c), the user buys a ticket but wants to activate later. In this case the ticket is stored in another folder that contains all tickets that are paid but not activated. The distinction between these tow folders and the respective actions are discussed in a latter section. In

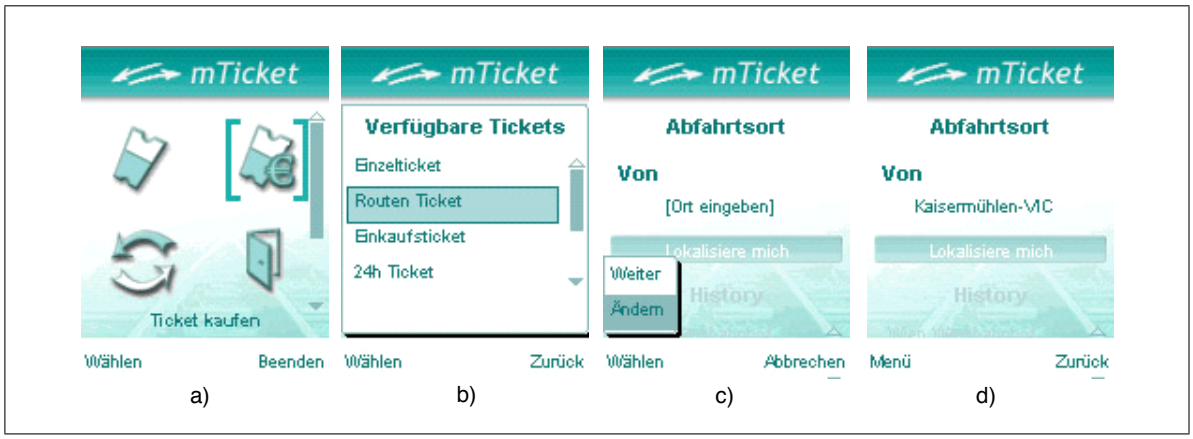

Figure 6.4: User Enters Departure Station by Hand

principle, the option to activate tickets immediately as they are bought saves users time when they are about to use a public transport. Tickets that are bought ahead give users more flexibility, for instance if they want to hand tickets over to other persons who are not allowed to buy tickets, e.g. kids.

Before the user proceeds to initiate the transaction, the application first requests the respective ticket price from application server. Upon receipt the mobile terminal application displays to the user all the details about the upcoming transaction which includes the number and price and if the ticket(s) are immediately activated or not. By pushing the left button, the buy process is initiated. At this point it is also necessary to enter the password to ensure that the mobile was not stolen or unwittingly used by another person. The application server receives the payment request and checks the user's payment account. If the amount of money available is not high enough, the transaction is halted and the user is informed to charge the account. If the transaction was performed successfully, the user's account is charged and the mobile application informs the user about the successful transaction.

6.1.4 Configuration of a Route Ticket

The route ticket allows users to first define a departure and arrival station. Based on that then the system calculates the best possible route, that is, the shortest sequence of public transports between the two denoted stations. A route consists of at least one transport, for example a certain underground train, up to several connected transports. Information about the route may further be used to provide additional information to users while on transit. We will discuss this later and continue so far with an explanation on how tickets can be configured on a mobile device.

When a user selects the route ticket she is provided with two possible ways to enter the departure station. One is to enter the destinations manually which is shown in figure 6.4 (c) where the menu point "*Ändern*" allows users to type in the desired station. The icon labelled (d) shows the manually selected station that is in this case *Kaisermühlen-VIC*.

The second possible way that is perhaps more convenient especially if one is not so familiar with the surrounding area is to select the option which provides a list of nearby stations that

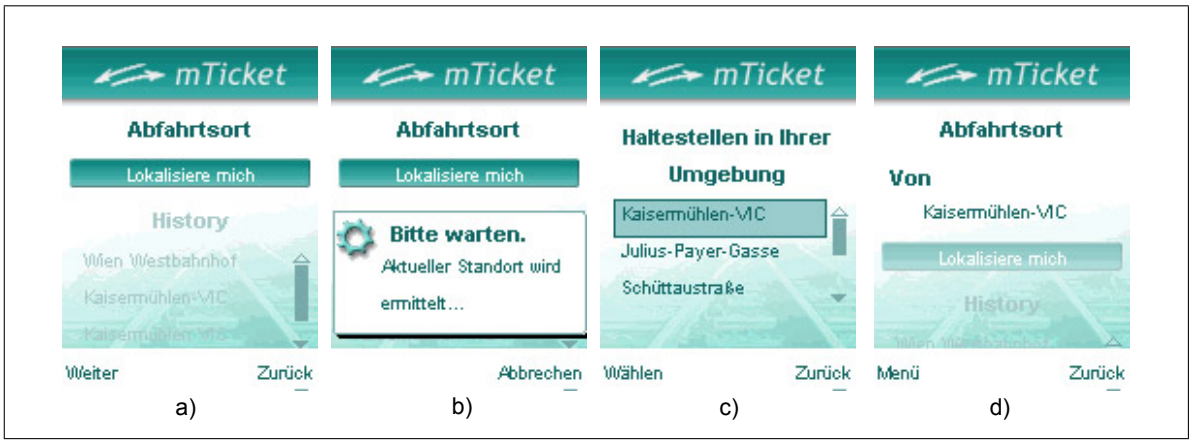

Figure 6.5: User Enters Departure Station by Localization

are determined by means of localization. The interaction sequence is depicted in figure 6.5. By selecting the option *Localisiere mich* (*localize me*) (see figure 6.4 (c)) the network operator's capability to localize the users is activated. The received location information is then passed to the dedicated route service which returns a set of nearby stations. In figure 6.5 the third icon (c) shows the three received nearby stations. The user may now select one out of these as his departure.

This feature not only releases mobile users from the burden to enter the name of the station manually. It further reduces typos and hence enhances the usability of the system. Another alleviation is that each entered station is stored on the mobile in a history file. This allows users to chose those stations that were already selected before instead of recurring inputs of the same stations. In addition to that it would also be feasible to recall previously stored routes.

Message Interaction for Position-fixing and determination of nearby stations

In the following we describe some important message interactions that allow users to determin their current position which in turn is used to retrieve those stations that come into question. The location information is determined by means of the network operator's localization technologies. It thus requires no additional interaction of the users. The location information is passed to a service provider which may calculate the nearby stations. The description assumes that the pseudonym generation scheme is already in use for identification purposes. At the time of writing this dissertation, the implementation of the transport ticket prototype does not integrate the pseudonym scheme as a means for identification. Thus, the following description is rather a conceptual thought whose implementation can be made up later.

When the user choses the *Lokalisiere mich* (*localizee me*) option shown as pictogram, message `locateCustAndFindNearestStation(.)` (see first message in figure 6.6) is sent together with a self identifying $pseudonym_{self}$ to the application server of the respective transport ticket provider. The request is then forwarded to the network operator's location service which first initiates a translation of the received pseudonym. Based on the identity information that is necessary to determine the actual location of the requesting users it sends

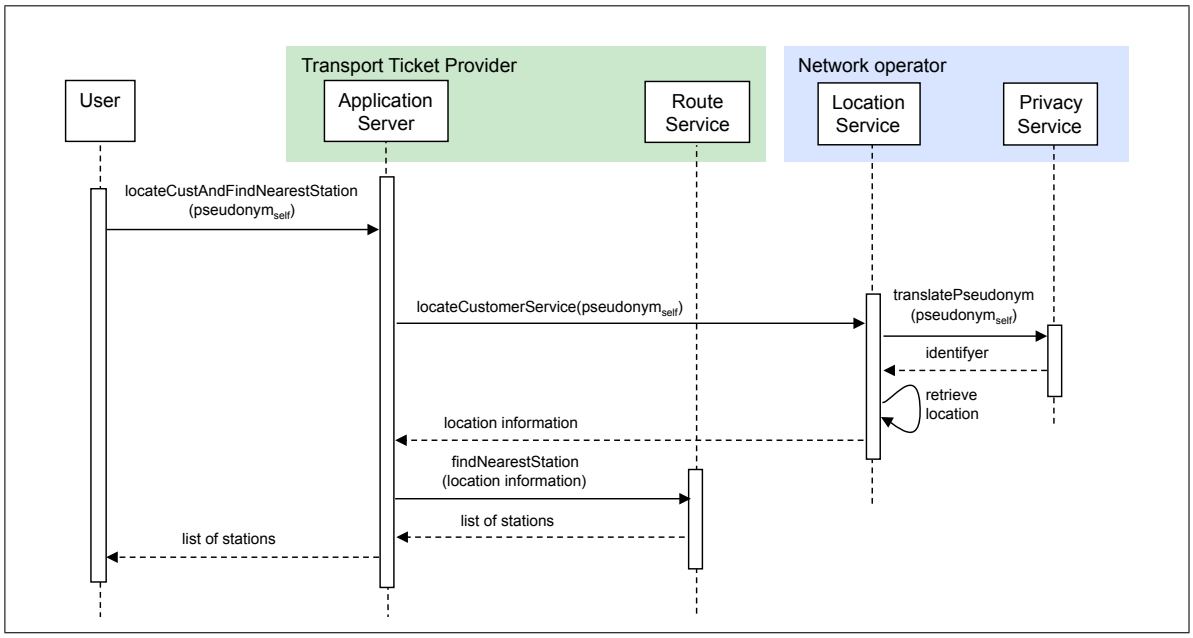

Figure 6.6: User receives Nearby Stations

the retrieved location information back to the transport tickets' application server which has access to a dedicated route service and provides a multitude of functions. One is route calculation which is described in the following subsection and delivers the list of stations. Finally, the route can be presented on the mobile terminal.

Message Interactions for Route Ticket Requests

As the user proceeds with "*Weiter*" (cf. figure 6.7 (b)), both the departure and the destination stations are passed to the transport ticket provider's application server. The request is processed by the route service which returns a list of possible routes the user may subsequently chose from. An example of a received numbered list of routes is depicted in figure 6.7 (d). The list of returned routes provides an overview which includes the departure and arrival time.

Users may now select one route and retrieve route details by selecting the option "*Details*". The detailed view of a route shows users information such as which kind of transport to enter, its identifier, the time when it is leaving, the name of the station from where it is leaving and the end station terminal. Little icons help to better pick up this information. The detailed route view does not contain each and every station but only those stations that are interception points of different transports including the departure and arrival stations. For each such station users may further request the respective map that shows the surrounding area of a station. Dedicated URIs are stored by the route service for a certain period of time. Each such URI points to a certain picture. As soon as routes are no longer accessed they are deleted after some minutes.

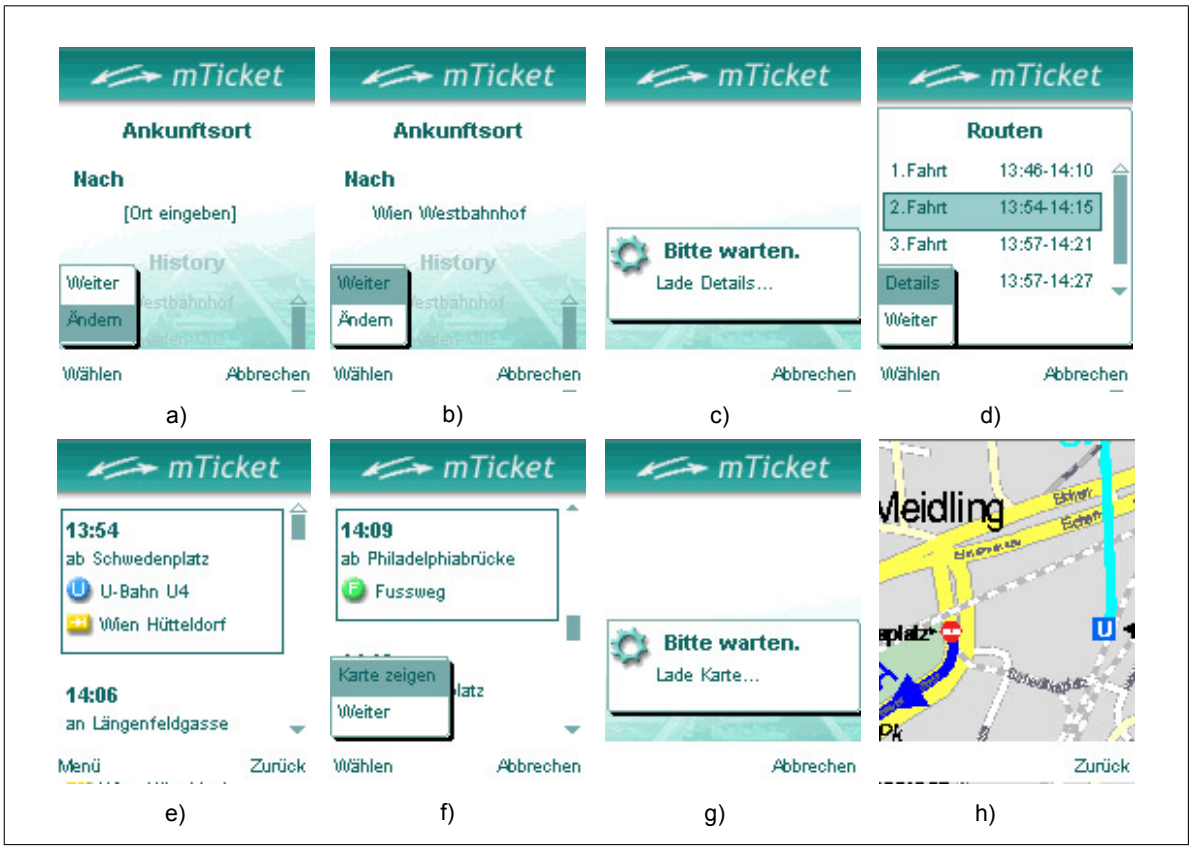

Figure 6.7: Route Configuration

Providing also pictures as an additional feature of the route details is of special importance in case when the connection between two transports requires users to walk along a footway. An example of such a route that contains a footway between two stations is shown in figure 6.7 (h).

6.1.5 Route Ticket Example with enabled Tracking Function

At the time of writing this dissertation the following feature is indeed not part of the transport ticket prototype. Beside the pseudonym generation scheme, the integration of the functionality of the tracking platform represents an additional advance that shows how aspects of location-based services may become part of applications that are used on an every-day basis. The the tracking functionality is discussed throughout this dissertation in various chapters under different viewpoints. The aim of this section is to show how the tracking functionality can be deployed as part of the transport ticket application. Thus, the following explanations indeed refer to the existing tracking platform but show rather an "*as-if*" example of a route ticket that integrates processing of location information.

The discussion about the possible integration of localization and tracking follows up the descriptions above which so far covers the configuration and generation of a so called route ticket. We assume that the user has selected and activated the ticket. This further includes

Figure 6.8: Visited Underground Stations (U1) in Vienna [12]

the processing of pseudonyms and the activation of the tracking functionality. The network operator's location service triggers a localization process whereupon the transport ticket application is notified about each location change of that particular user. For a more detailed discussion regarding the localization strategy we refer to section 5.7.2 (p. 145).

Each received location update is assigned to its respective route ticket that in turn belongs to a dedicated user. Depending on the respective implementation at hand, the transport ticketing application may use the user's position information and based on that provide additional added value such as when the next transport arrives, the elapsed time and so on. Even though the ticketing application does not dispose of any of the user's contact details, it may anyhow notify users about certain location and context related conditions. Since each active route ticket is associated with a dedicated session identifier that is administered by the transport ticket provider and the network operator's privacy service likewise, this allows the network operator to retrieve the user's identifying information such as e.g. the MSISDN based on that particular session identifier. Thus, network operators may also convey notification messages to the respective user. One benefit that turns out of this solution is that notifying users is possible even without harming the user's privacy and much additional communication or processing overhead.

Figure 6.8 shows the positions that are evaluated by the network operator's location service while one user travels by underground. In this particular case, the locations match with the locations of the underground stations because the network in operation provides dedicated antennas in each underground station to guarantee better radio reception. As the locations of transport stations do not necessarily match the locations of different network operators antennas, the shown picture presents rather the ideal case. In fact, the locations received from the network operator mainly depend on the network plan, which is certainly different for each operator.

As for most cases it can be assumed that the user's location cannot be displayed as perfectly as it is depicted in figure 6.8. It is much more likely that most show location variances. But, for provisioning the ticket transport application this does not necessarily play an important

role nor a problem. It is rather very likely that in the majority of cases the transport network does not reflect the mobile antenna network as it is shown in figure 6.8. Thus, an analysis of the traffic flow would be an important precondition to adjust the transport ticket application according the the respective network related conditions.

6.2 Summary

The mobile transport ticket application demonstrator presented in this section is only one out of many possible examples that shows how existing mobile applications such as the existing transport ticket may be further extended by the integration of location information. The inclusion of location information enables application providers to provide advanced functionalities to ther customers which increases ease of use and further the acceptance of such applications. Therefore, the inclusion of location information requires proper protection mechanisms in order to be able to guarantee user's location privacy and security. Such solutions are challenged to conform with changing technical and legal framework conditions and thus have to be flexible enough to be adapted according such changes.

The finally presented ticket application shows not only what kind of features and possibilities advanced mobile ticket application may provide to users. It further reveals what additional requirements have to be considered to provide large-scale location-based applications.

Articles

The following article contributed to this section:

3. Oliver Jorns, Gerald Quirchmayr: A Privacy Enhancing Mechanism for Mobile Tickets using Telecommunication Services, In Applied Information Technology Research - Articles by Cooperative Science Network, University of Lapland, Department of Research Methodology Reports, Essays and Working Papers, Juha Lindfors (ed.), ISBN 952-484-046-4, ISSN 1796-4474, Rovaniemi, Finland, 2007

11. Oliver Jorns, Gerald Quirchmayr. A Transport Ticket System with Location and Privacy Protection, 6th Eastern Europe eGov Days, April 23-25, 2008, Prague, CZ

Article 3 discusses the system architecture and its components that are necessary for the realization of a ticket application with special focus on the ticket format and secure payment.

Article 11 discusses how existing large-scale mobile applications such as the transport ticketing application can be enhanced by the inclusion of location information. This example is representative for a whole new class of mobile applications that collect, process and exchange location information.

Chapter 7

Conclusions and Future Work

During the last decade bulky mobile phones have turned into powerful pocket size computers. This development has also rung in a renaissance of Location-Based Services and the development of applications that process location information. Research in the field of Location-Based Services is of utmost interest for many researchers and practitioners from different disciplines. In this respect, one of the most challenging issues researchers and practitioners have to face is how to maintain security and privacy while sensitive data is exchanged. This involves the design, implementation and verification of different communication protocols, different networks, consideration of models and communication patterns as well as a variety of different systems that are subject to further development.

We identified research efforts in security and privacy protections in the field of mobile computing and location-based services and applications as to be one of the most important research directions in this area. Research in this field is not restricted to certain technical aspects only. On the contrary, it concerns almost every aspect, be it from a technical, legal and social point of view. With the continuing proliferation of the world wide web and the accompanying development of mobile devices which provide advanced communication, presentation and computational capabilities and allow instant access to almost any information from any place, mobile computing continues to deregulate place bound computing. By adjoining location information the development of location-based services and applications as we can see it today is indeed still at its early stages. A decade ago, at the beginning of this development path, the idea of location-based services raised sweeping expectations in high revenues. The first who adopted this idea and provided the first location-based services were mobile operators. However, only a few years later many of them came to the conclusion that the success of location-based services belied in these high expectations. The main reasons were the missing customer's acceptance of these technologies, immature technologies and applications and, most important, missing user's trust in exchanging the location information. In the meantime, the situation has partially changed. Although many users are still hesitant in providing or sharing their location information with other users or service providers, there are also numerous examples showing that under certain circumstances users are quite willing to trade their private information against services. This contradictory situation and the noticeable proliferation in the area of mobile computing clearly demonstrate the importance of appropriate means that aim for security and privacy protection of users.

We proposed a pseudonym generation scheme that can be applied by a dedicated service architecture. By bringing together two different worlds this contributes to the ongoing evolution in mobile networks and beyond that represents an important step towards privacy protection in the area of location-based services. On the one hand our proposed solution enables service providers to participate in a trusted network operator's domain and provide better services with much more value. On the other hand, network operators take part of highly dynamic developments without the need of high investments and risks. This bilateral approach allows for the implementation of new business models which provides new possibilities of revenues by still protecting the user's identities.

The, use of mobile network operator's resources for the development of location-based services provides not only a number of opportunities but also limits. Depending on the respective application at hand, there are social, technological and legal restrictions network operators, application developers and users have to face. Throughout this dissertation we discussed a number of these limitations.

Future Work

The question: *"Who should have access to what location information under which circumstances?"* is the core question to our next research. J. Zeiss and O. Jorns propose in [162, 178] the use of human readable policies as extension to the system discussed in this dissertation. Therefore, the use of semantic web technologies eases the definition and use of policies through a common vocabulary, provides a way to declare data and their meaning and allows the processing of it with inference mechanisms. This refers to the requirement as they occur in ubiquitous computing environments where conditions may change according to changing environments. Thus, instead of using account-based privacy protection mechanisms this approach extends the proposed pseudonym based scheme that can solely be used for authentication and identification of identities by dynamic expressions that can be adopted to changing environments without the need of human intervention.

Bibliography

[1] Einführung GSM / DCS. Siemens, Bereich Öffentliche Kommunikationsnetze ÖN SU, Sachnummer P30181-X1760-X200-1, 1995.

[2] Stefan Figge and Kai Rannenberg. Inviting new Players to the Multimedia M-Commerce Area - An approach to enhance the current M-Commerce business model with regard to merging DVB-T networks. In Elaine Lawrence, Barbara Pernici, and John Krogstie, editors, *Working Conference on Mobile Information Systems (MOBIS)*, volume 158 of *IFIP International Federation for Information Processing*. Mobile Information Systems; Spinger, New York, September 2004.

[3] H. Maurer, Tilo Balke, Frank Kappe, Narayanan Kulathuramaiyer, Stefan Weber, and Bilal Zaka. Report on dangers and opportunities posed by large search engines, particularly Google. Technical report, Institute for Information Systems and Computer Media, Graz University of Technology, 2007.

[4] Marie Antoinette Online. URL: http://www.marie-antoinette.org, last viewed 8. Aug. 2009.

[5] A. J. Menezes, P.C. Van Oorschot, and S.A Vanstone. *Handbook of Applied Cryptography*. CRC Press series on discrete mathematics and its applications, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, 1996.

[6] FIPS PUB 198, Federal Information Processing Standards Publication, The Keyed-Hash Message Authentication Code (HMAC), Information Technology Labratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, March 6, 2002.

[7] Leslie Lamport. Password Authentication with Insecure Communication. In *Communications of the ACM*, volume 24(11), pages 770–772, 1981.

[8] Farooq Anjum and Petros Mouchtaris. *Security for Wireless Ad Hoc Networks*. 978-0-471-75688-0. WILEY, 2007.

[9] Oliver Jorns, Gerald Quichmayr, and Oliver Jung. A Privacy Enhancing Mechanism based on Pseudonyms for Identity Protection in Location-Based Services. In *Australasian Information Security Workshop (Privacy Enhancing Technologies) AISW-PET2007 at the Australasian Computer Science Conference in Ballerat, Victoria, Australia*, 2007.

[10] Oliver Jorns, Oliver Jung, and Gerald Quirchmayr. A Platform for the Development of Location-Based Mobile Applications with Privacy Protection. In *The 3rd International Conference on COmmunication System softWAre and MiddlewaRE (COMSWARE 2008), Bangalore, India*, January 6-10, 2008.

[11] Oliver Jorns and Gerald Quirchmayr. A Middleware for Location-Based Mobile Applications. In *10th International Conference on Information Integration and Web-based Applicatoin & Services (iiWAS2008), Linz, Austria*, November 24-26.

[12] Oliver Jorns and Gerald Quirchmayr. A Transport Ticket System with Location and Privacy Protection. In *6th Eastern Europe eGov Days, Prague, CZ*, April 23-25, 2008.

[13] Directive 2002/58/EC of the European Parliament and of the Council concering the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). In *Official Journal of the European Communities L 201/37*, 2002.

[14] Mika Raento. *Exploring privacy for ubiquitous computing.* PhD thesis, University of Helsinki, Department of Computer Science, 2007.

[15] Nikita Borisov, Ian Goldberg, and Eric Brewer. Off-the-Record Communication, or, Why Not To Use PGP. In *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, WPES 2004, Washington, DC, USA*, pages 77–84, October, 28 2004.

[16] Rasmus L. Olsen, Hans-Peter Schwefel, and Martin B. Hansen. Quantitative Analysis of Access Stategies to Remote Information in Network Services. In *Global Telecommunications Conference, CLOBECOM 2006 - IEEE*, 2006.

[17] Albrecht Schmidt, Michael Beigl, and Hans-W. Gellersen. There is more to Context than Location. *Computers and Graphics*, 23(6):893–901, 1999.

[18] Daniel Salber, Anind K. Dey, and Gregory D. Abowd. The Context Toolkit: Aiding the Development of Context-Enabled Applications. In ACM Press, editor, *ACM Conference on Human Factors in Computing Systems (HCI'99)*, pages 434–441, May 1999.

[19] Gregory D. Abowd and Elizabeth D. Mynatt. Charting Past, Present, and Future Research in Ubiquitous Computing. In *ACM Transaction on Computer-Human Interaction (TOCHI)*, pages 29–58, March 2000.

[20] Jonathan Raper, Georg Gartner, Hassan Karimi, and Crhis Rizos. A Critical Evaluation of Location Based Services and their Potential. *Journal of Location Based Services*, 1(1):5–45, March 2007.

[21] Mark Weiser. The Computer for the Twenty-First Century. In *Scientific American*, pages 94–100, September 1991.

[22] Hans-Werner Gellersen, editor. *Handheld and Ubiquitous Computing, First International Symposium, HUC'99, Karlsruhe, Germany, September 27-29, 1999, Proceedings*, volume 1707. Springer, 1999.

[23] René Mayrhofer. *An Architecture for Context Prediction*. PhD thesis, Johannes Kepler University of Linz, Austria, October 2004.

[24] Thomas Erickson. Some Problems with the Notion of Context-Aware Computing. In *Communications of the ACM*, volume 45, pages 102–104, 2002.

[25] Alan Dix, Tom Rodden, Nigel Davies, Jonathan Trevor, Adrian Friday, and Kevin Palfreyman. Exploiting Space and Location as a Design Framework for Interactive Mobile Systems. *ACM Transactions on Computer-Human Interaction*, 7(3):285–321, September 2000.

[26] Guanling Chen and David Kotz. A Survey of Context-Aware Mobile Computing Research. Technical report, Department of Computer Science, Dartmouth College, 2000.

[27] Anind K. Dey and Gregory D. Abowd. Towards a Better Understanding of Context and Context-Awareness. In *Workshop on The What, Who, Where, When, and How of Context-Awareness, as part of the 2000 Conference on Human Factors in Computing Systems (CHI 2000), The Hague, The Netherlands, April 3, 2000. Also GVU Technical Report GIT-GVU-99-22. Submitted to the 1st International Symposium on Handheld and Ubiquitous Computing (HUC '99), June 1999.*, June 2000.

[28] P. J. Brown. The Stick-e Document: a Framework for Creating Context-aware Applications. In *Proceedings of EP'96, Palo Alto*, pages 259–272. also published in it EP–odd, January 1996.

[29] Roy Want, Andy Hopper, Veronica Falão, and Jonathan Gibbons. The Active Badge Location System. *ACM Transactions on Information Systems*, 10(1):91–102, 1992.

[30] Sue Long, Dietmar Aust, Gregory D. Abowd, and Chris Atkeson. Cyberguide: Prototyping Context-Aware Mobile Applications. In *CHI'96 short paper*, 1996.

[31] Sue Long, Rob Kooper, Gregory D. Abowd, and Christopher G. Atkeson. Rapid Prototyping of Mobile Context-Aware Applications: The Cyberguide Case Study. In *Proceedings of the 2nd ACM International Conference on Mobile Computing and Networking (MobiCom'96)*, 1996.

[32] Gregory D. Abowd, Christopher G. Atkeson, Jason Hong, Sue Long, Rob Kooper, and Mike Pinkerton. Cyberguide: A Mobile Context-Aware Tour Guide. In *Baltzer/ACM Wireless Networks*, volume 3, 1997.

[33] Natalia Marmasse and Chris Schmandt. Location-Aware Information Delivery with ComMotion. In *Second International Symposium on Handheld and Ubiquitous Computing (HUC 2000)*, pages 157–171. Springer, 2000.

[34] Ulf Leonhardt. *Supporting Location-Awareness in Open Distributed Systems*. PhD thesis, Department of Computing, Imperial College of Science, Technology and Medicine, University of London, May 1998.

[35] Barry Brown, Alex S. Taylor, Shahram Izadi, Abigail Sellen, Joseph Kaye, and Rachel Eardley. Locating Family Values: A Field Trial of the Whereabouts Clock. In London Lecture Notes In Computer Science. Springer-Verlag, editor, *Proceedings of the 9th international Conference on Ubiquitous Computing (Ubicomp'07), Innsbruck, Austria*, September 2007.

[36] Asaf Burak and Taly Sharon. Usage Patterns of FriendZone - Mobile Location-Based Community Services. In ACM International Conference Proceeding Series, editor, *Proceedings of the 3rd international conference on Mobile and ubiquitous multimedia*, volume 83, pages 93–100, 2004.

[37] Axel Küpper and Georg Treu. *Next Generation Location-based Services - Merging Positioning and Web 2.0.* John Wiley & Sons, March 2008.

[38] Peter Dibdin. Where are mobile location based services? *CM316 Multimedia Systems Paper*, December 2001.

[39] Kou-Chen Wu and Lir-Fan Sun. A Self-Served Mobile Location Query Service. *Intelligent Network Workshop*, 2001.

[40] Iris A. Junglas and Christiane Spitzmüller. A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services. In *Proceedings of the 38th Hawaii International Conference on System Sciences, HICSS '05*, 2005.

[41] K. Adusei, I. K. Kaymakya and F. Erbas. Location-based services: Advances and challenges. In *CCECE 2004, CCGEI 2004*. IEEE, May 2004.

[42] Axel Küpper. *Location-based Services Fundamentals and Operation.* John Wiley and Sons, 2005.

[43] George M. Giaglis, Panos Kourouthanasis, and Argirios Tsamakos. *Mobile Commerce: Technology, Theory, and Applications, Towards a Classification Framework for Mobile Location Services*, chapter IV, pages 67–85. ISBN 1591400449. Idea Group Publishing, 2003.

[44] Bernhard Walke. *Mobilfunknetze und ihre Protokolle 1.* B. G. Teubner Stuttgart Leipzig Wiesbaden, 3rd edition, August 2001.

[45] Matt Duckham and Lars Kulik. A Formal Model of Obfuscation and Negotiation for Location Privacy. In *Pervasive Computing, Third International Conference, PERVASIVE 2005*, pages 152–170. Springer, Lecture Notes in Computer Science, 2005.

[46] Rainer Simon, Peter Fröhlich, Gerhard Obernberger, and Erwin Wittowetz. The Point to Discover GeoWand. In *Proceedings of the 9th International Conference on Ubiquitous Computing (UbiComp 07).* Innsbruck, Austria, September 16-19 2007.

[47] Bill Schilit, Jason Hong, and Marco Gruteser. Wireless Location Privacy Protection. In *IEEE Computer*, pages 135–137, 2003.

[48] Veljo Otsason. Accurate Indoor Locatlization using Wide GSM Fingerprinting. Master's thesis, University of Tartu, Faculty of Mathematics and Computer Science, 2005.

[49] Stefanie Richter and Andreas Böhm. A Location and Privacy service enabler for context-aware and location-based services in ngn. In *12th International Telecommunications Network Strategy and Planning Symposium, 2006. NETWORKS 2006.*, 2006.

[50] K. Kyamakya, M. Khalaf-Allah, A. Popovic, and B. Lamprecht. Ortungssysteme in der Transportlogistik: Schnell und sicher reagieren. *MM Logistics*, 2006.

[51] Ahmed El-Rabbany. *Introduction to GPS*. Artech House, 2002.

[52] IEEE 802.15 WPAN Task Group 1 (TG1), URL: http://www.ieee802.org/15/pub/TG1.html (last visited 12. Jannuary 2009).

[53] Sandford Bessler. Lokalisation mittels Bluetooth-Beaken. Patent Nr. AT 504139, Österreichisches Patentamt, August 2006.

[54] Pasquale Pace, Gianluca Aloi, and Antonio Palmacci. New Wireless Communication Architectures for Interactive Fruition of Historical and Artistic Contents. In *1st IFIP Wireless Days Cconference, Dubai, United Arab Emirates*, November 24-27, 2008.

[55] Harald Laimer. Visualisierung von Verkehrszuständen mittels Floating Car Daten. master thesis, Technikum Wien, Fachhochschulstudiengang Elektronik, February 2005.

[56] Louise Barkhuus and Anind K. Dey. Location-Based Services for Mobile Telephony: a study of users' privacy concerns. In *Interact 2003*, Zurich, CH, 2003. ACM Press.

[57] Axel Küpper, Georg Treu, and Claudia Linnhoff-Popien. Trax: A Device-Centric Middleware Framework for Location-Based Services. In *IEEE Communications Magazine*, volume 44, pages 114–120, September 2006.

[58] Paolo Bellavista, Axel Küpper, and Sumi Helal. Location-Based Services: Back to the Future. In *IEEE Pervasive Computing*, volume 7(2), April - June 2008.

[59] Diana Weiß, Isabelle Krämer, Georg Treu, and Axel Küpper. Zone Services - An Approach for Location-Based Data Collection. In *CEC-EEE '06: Proceedings of the The 8th IEEE International Conference on E-Commerce Technology and The 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services*, 0-7695-2511-3, page 79, Washington, DC, USA, 2006. IEEE Computer Society.

[60] Marco Gruteser and Xuan Liu. Protecting Privacy in Continuous Location-Tracking Applications. *IEEE Security and Privacy*, 2004.

[61] Emergency Telecommunications (EMTEL). URL: http://www.emtel.etsi.org/ (last visited 13. January 2009).

[62] Werner Kurschl, Stefan Mitsch, Johannes Schönböck, and Wolfgang Beer. Modeling Wireless Sensor Networks based Context-Aware Modeling Wireless Sensor Networks

based Context-Aware Emergency Coordination Systems. In *Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services*. ACM, November 2008.

[63] Frank Ohrtman. *WiMAX Handbook Building 802.16 Wireless Networks*. McGraw-Hill Communications, 2005.

[64] Frank Ohrtman. *WiMAX in 50 Pages*. WMX Systems, 2006.

[65] Alesander Osterwalder, Jan Ondrus, and Yves Pigneur. Skype's Disruptive Potential in the Telecom Market: A Systematic Comparison of Business Models, May 2005.

[66] Marc Levinson. *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger*. Princeton University Press, 2006.

[67] Gerald Reischl. *Die Google Falle*. Ueberreuter Verlag, 2008.

[68] Gerald Quirchmayr and Christopher C. Wills. Data protection and Privacy laws in the light of RFID and emerging technologies. In *Trust, Privacy and Security in Digital Business, 4th International Conference, TrustBus 2007, Regensburg, Germany*, 2007.

[69] Matt Duckham and Lars Kulik. Location Privacy and Location-Aware Computing. In *Dynamic & Mobile GIS: Investigating Change in Space and Time*, pages 34–51. CRC Press: Boca Raton, Florida, USA, 2006.

[70] Martin Colbert. A Diary Study of Rendezvousing: Implications for Position-Aware Computing and Communications for the General Public. In *Proceedings of the 2001 International ACM SIGGROUP Conference on Supporting Group Work*, pages 15–23, 2001.

[71] Louise Barkhuus, Barry Brown, Marek Bell, Malcolm Hall, Scott Sherwood, and Matthew Chalmers. From Awareness and Repartee: Sharing location within Social Groups. In *CHI 2008, Florence, Italy*, April 2008.

[72] Louise Barkhuus. Concern vs. Privacy in Location-Based Services, Concern vs. Coolness. In *Workshop paper in Mobile HCI 2004 workshop: Location System Privacy and Control*, 2004.

[73] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. In *IEEE Pervasive Computing*, volume 2, pages 45–55, 2003.

[74] S. Consolvo, I.E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location Disclosure to Social Relations: Why, When, & What People Want to Share. In *Proceedings of the Conference on Human Factors and Computing Systems: CHI '05, Portland, Oregon*, pages 81–90, April 2005.

[75] Rainer Simon, blogloc URL: http://geekvault.no5.at/blogloc/index.jsp (last checked: 22. November 2008).

[76] Strategy Analytics, Adobe Systems Incorporated, Understanding the Mobile Ecosystem, A White Paper Prepared for Adobe Systems Incorporated, January 2008.

[77] NTT DoCoMo, DoCoMo Newsletter "Mobility"
URL: http://www.nttdocomo.com/about/publications/mobility/index.html (last visited 4. April 2009), April 2008.

[78] Ragnar Schierholz. *Mobile Kundeninteraktionen bei Dienstleistungsunternehmen.* PhD thesis, University of St. Gallen, 2007.

[79] Heise online, EU-Parlament gibt grünes Licht für Galileo, URL: http://www.heise.de/newsticker/eu-parlament-gibt-gruenes-licht-fuer-galileo–/meldung/106925 (last visited 17. May 2008), April 2008.

[80] Ramaprasad Unni and Robert Harmon. Location-Based Services: Models for Strategy Development in M-Commerce. In *Portland International Conference on Management of Engineering and Technology (PICMET'03) Technology Management for Reshaping the World*, 2003.

[81] Giovanni Camponovo and Yves Pigneur. Business Model Analysis Applied to Mobile Business. In *International Conference on Enterprise Information SystemS, ICEIS'2003*, 2003.

[82] Otto Petrovic, Christian Kittl, and Ryan D. Teksten. Developing Business Models for Ebusiness. In *International Conference on Electronic Commerce*, 2001.

[83] Adrian J. Slywotzky. *Value Migration: How to Think Several Moves Ahead of the Competition.* Harvard business Harvard Business School Press, 1995.

[84] Andy Tiller. The Case for Femtocells Operator Business Case and Consumer Propositions. whitepaper V1.1, ip.access, 2007.

[85] The Parlay X 2.0 Specification, URL: http://www.parlay.org/en/specifications/ (last visited 4. April 2009).

[86] Alan F. Westin. *Privacy and Freedom.* Atheneum, New York, USA, 1967.

[87] Charles P. Pfleeger and Shari Lawrence Pfleeger. *Security in Computing.* Prentice Hall, 4 edition, 2007.

[88] Privacy and Human Rights. URL: http://www.gilc.org/privacy/survey/ (last visited: 27. November 2007).

[89] The History of Justices of the Peace (Magistrates), URL: http://www.hmcourts-service.gov.uk/aboutus/history/magistrates.htm (last visited 1. February 2008), February 2008.

[90] William Pitt. Historical Sketches of Statesmen Who Flourished in the Time of George III, URL: http://www.bartleby.com/73/861.html (last visited 4. April 2009). In *Speech in the House of Lords, 1763*, volume 1, page 52, 1763.

[91] Samuel D. Warren and Louis D. Brandeis. The Right to Privacy. *Harvard Law Review*, 4(5):193–220, December 1890.

[92] Land Hessen Federal Republic of Germany (1970): Data Protection Act of 7 October 1970.

[93] Adam Warren. Right to privacy? The protection of personal data in UK public organisations. In *New Library World*, pages 446–456, 2002.

[94] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In *Official Journal of the European Communities L 281/31*, 1995.

[95] Baine A. Price. The Law is Not Enough: Legislation and Privacy Enhancing Technology for Location-Aware Computing. In *Workshop on Location Systems Privacy and Control, Held at MobileHCI 04*, September 13 2004.

[96] S. Fischer-Hübner. *IT-Security and Privacy.* LNCS 1958. Springer-Verlag Berlin Heidelberg, 2001.

[97] Directive 2006/24/EC of the European Parliament and on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. In *Official Journal of the European Communities*, 2006.

[98] Gerald Quirchmayr and Christopher C. Wills. Some thougts on the legal background of the continously increasing privacy risk in information systems and how to deal with it. In *3rd International Conference, EC-Web 2002 - Aix-enProvence, France*, 2002.

[99] Rupert Thorogood and Charles Brookson. Lawful interception. *Telektronikk, Privacy in Telecommunications*, 2007.

[100] Berit Svendsen. The EU Directive on Data Retention - An End to Justify the Means. *Telektronikk, Privacy in Telecommunications*, February 2007.

[101] Dillip Mohapatra and Suma S.B. Survey Of Location Based Wireless Services. In *Personal Wireless Communications. ICPWC'05*, 2005.

[102] Java Community Process JSR-179 Expert Group. *Location API for Java 2 Micro Edition*, 2003.

[103] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol, RFC 3261, 2002.

[104] 3GPP TS 22.228, Internet Protocol (IP) Multimedia Core Network Subsystem; Stage 1.

[105] 3GPP TS 23.228, IP Multimedia Subsystem (IMS); Stage 2.

[106] Marco Happenhofer, Joachim Zeiss, Rene Gabner, and Sandford Bessler. Signalling HTTP Sessions in the IP Multimedia Subsystem using SIP - Architecture and Services. In *The Fourth International Wireless Internet Conference (WICON 2008)*, 2008.

[107] Open Mobile Alliance, Mobile Location Protocol V3.1: http://www.oma-works.org/technical/release_program/mlp_v31.aspx (last visited 6. August 2008).

[108] OMA (Open Mobile Alliance): http://www.openmobilealliance.org/ (last visited 1. march 2009).

[109] Shu Wang, Jungwon Min, and Byung K. Yi. Location Based Services for Mobiles: Technologies and Standards. In *IEEE International Conference on Communication (ICC), Beijing, China*, 2008.

[110] Marco Gruteser and Dirk Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *International Conference on Mobile Systems, Applications and Services*. ACM Press, 2003.

[111] IETF Geographic Location/Privacy: http://www.ietf.org/html.charters/geopriv-charter.html (last visited 22. July 2008).

[112] Electronic Privacy Information Centre (EPIC): The Public Voice URL: http://thepublicvoice.org/ (last visited 24. January 2008).

[113] Electronic Privacy Information Center: http://epic.org (last visited 24. January 2008).

[114] Parliament of the United Kingdom: Data Protection Act 1998 (c.29) URL: http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1 (last visited 24. January 2008).

[115] ATIS TELECOM GLOSSARY 2000, ATIS Committee T1A1, Performance and Signal Processing, URL: http://www.atis.org/tg2k/_signaling.html (last visited 25. January 2008).

[116] Geir M. Køien and Vladimir A. Oleshchuk. Personal Privacy in a Digital World. In telektronikk 2.07, editor, *Privacy in Telecommunications*, volume 103, pages 4–19, 2007.

[117] J. Grimson. Delivering the Electronic Healthcare Record for the 21st Century. In *International Journal of Medical Informatics*, volume 2, pages 111–127, 2001.

[118] Bernhard Riedl, Veronika Grascher, and Thomas Neubauer. A Secure e-Health Architecture based on the Appliance of Pseudonymization. In *Journal of Software*, volume 3, pages 23–32, 2008.

[119] Bernhard Riedl and Oliver Jorns. Secure Access to Emergency Data in an e-Health Architecture. In *The Ninth International Conference on Information Integration and Web-based Applications Services (iiWAS'2007)*, volume 229, pages 297–306, 2007.

[120] Roman Schlegel, Saverio Niccolini, Sandra Tartarelli, and Marcus Brunner. Spam over internet telephony (spit) prevention framework. In *Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE*, 2006.

[121] J. Quittek, S. Niccolini, S. Tartarelli, M. Stiemerling, M. Brunner, and T. Ewald. Detecting SPIT Calls by Checking Human Communication Patterns. In IEEE, editor, *ICC '07. IEEE International Conference on Communications*, pages 1979–1984, June 2007.

[122] Martin Herfurt. Bluesnarfing @ cebit 2004. Technical report, Salzburg Research Forschungsgesellschaft, mbH, March 30. 2004.

[123] Martin Petraschek. Bluetooth security. Technical Report FTW-TR-2006-002, ftw. Telecommunications Research Centre Vienna, January 2006.

[124] Kjetil Rognsvåg. Privacy and Protection of Personal Data. *Telektronik, Privacy in Telecommunications*, February 2007.

[125] John Krumm. A Survey of Computational Location Privacy. In *5th International Workshop on Privacy in UbiComp (UbiPriv'07)*, pages 403 – 409. Springer, September 2007.

[126] Intel Research. Pols v1.1 (privacy-observant location system): Url: http://pols.sourceforge.net/ (last visited 7. june 2008).

[127] Marta C. Gonzalez, Cesar A. Hidalgo, and Albert-Laszlo Barabasi. Understanding individual human mobility patterns. *Nature*, 453(7196):779–782, 2008.

[128] Mohamed F. Mokbel. Towards Privacy-Aware Location-Based Database Servers. In *Second International Workshop on Privacy Data Management (PDM 2006)*, April 2006.

[129] Natalia Marmasse. *Providing Lightweight Telepresence in Mobile Communication to Enhance Collaborative Living*. PhD thesis, Massachusetts Institute of Technology, September 2004.

[130] Baik Hoh and Marco Gruteser. Protecting Location Privacy Through Path Confusion. In *First International Conference on Security and Privacy for Emergin Areas in Cummunication Networks (SecureComm'05)*, 2005.

[131] John Krumm. Inference Attacks on Location Tracks. In *Fifth International Conference on Pervasive Computing (Pervasive 2007), Toronto, Ontario, Canada*, May 13-16 2007.

[132] Marco Gruteser and Baik Hoh. On the Anonymity of Periodic Location Samples. In *Second International Conference on Security in Pervasive Computing (SPC'05)*, pages 179–192, Boppard, Germany, 2005.

[133] Latanya Sweeney. k-Anonymity: a model for protecting privacy. In *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, volume 10 (5), pages 557–570, 2002.

[134] R. Agrawal and R. Srikant. Privacy-Preserving Data Mining. In *ACM SIGMOD Conference on Management of Data, Dallas, TX, USA*, pages 439 – 450, 2000.

[135] Mika Raento and Antti Oulasvirta. Privacy management for social awareness applications. In *Proceedings of Workshop on Context Awareness for Proactive Systems (CAPS 2005)*, 2005.

[136] Rakesh Agrawal, Alexandre Evfimiesvski, and Ramakrishnan Srikant. Information Sharing Across Private Databases. In *Proceedings of the ACM International Conference on Management of Data, SIGMOD03*, 2004.

[137] Fatih Emekci, Divyakant Agrawal, Amr El Abbadi, and Aziz Gulbeden. Privacy Preserving Query Processing using Third Parties. In *Proceedings of the 22nd International Conference on Data Engineering*, 2006.

[138] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In August, editor, *Proceedings of the 13th USENIX Security Symposium*, 2004.

[139] Jason I. Hong and James A. Landay. An architecture for privacy-sensitive ubiquitous computing. In ACM Press, editor, *Proceedings of the 2nd International Conference on Mobile Systems, Applications and Services*, pages 177–189, 2004.

[140] Jalal Al-Muhtadi, Roy Campbell, Apu Kapadia, M. Dennis Mickunas, and Seung Yi. Routing through the mist: Privacy preserving communication routing Through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments. In *Proceedings of IEEE International Conference of Distributed Computing Systems (ICDCS)*, pages 65–74, Vienna, 2002.

[141] Andreas Pfitzmann and Marit Hansen. Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology. Anon Terminology Paper 0.28, TU Dresden, ULD Kiel, May 2006.

[142] David L. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In *Communications of the ACM*, volume 24(2), pages 84–90, February 1981.

[143] Einar Snekkenes. Concepts for personal location privacy policies. In *3rd ACM conference on Electronic Commerce*, pages 48–57. ACM Press, 2001.

[144] Reynold Cheng, Yu Zhang, Elisa Bertino, and Sunil Prabhakar. Preserving User Location Privacy in Mobile Data Management Infrastructures. In *Privacy Enhancing Technologies*, volume 4258/2006, pages 393–412. Springer Berlin / Heidelberg, 2006.

[145] Georg Treu and Axel Küpper. Datenschutzmechanismen für Ortsinformationen aus der Sicht zukünftiger Anwendungen. In *Tagungsband des zweiten GI/ITG KuVS Fachgesprächs über ortsbezogene Anwendungen und Dienste*, pages 66–71. Fernuniversität Hagen, Stuttgart, Germany, 2005.

[146] Mihir Bellare and Phillip Rogawayy. Random Oracles are Practical: A Paradigm for Designing Effcient Protocols. In *First Annual Conference on Computer and Communications Security, ACM*, 1993.

[147] National Institute of Standards and Technology, Data Encryption Standard (DES), Federal Information Processing Standards Publications 46-3, October 1995.

[148] National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publications 197. November 26, 2001.

[149] F. Bavaud, J.-C. Chappelier, and J.Kohlas. An Introduction to Information Theory and Applications. URL: http://diuf.unifr.ch/tcs/courses/it04-05/ (last viewed 23. March 2009), 2005.

[150] Bruce Schneier. *Applied Cryptography.* Pearson Studium, 2006.

[151] Network of Excellence in Cryptology IST-2002-507932. Recent collision attacks on hash functions. Position paper, ecrypt.eu.org, February 2005.

[152] M. Bellare, R Canetti, and H. Krawczky. Keying Hash Functions for Message Authentication. In *Lecture Notes in Computer Science*, volume 1109 of *Advances in Cryptology - CRYPTO'96*, pages 1–15. Springer, Heidelberg, 1996.

[153] M. Bellare, R Canetti, and H. Krawczky. Message Authentication using Hash Functions - The HMAC Construction. In *RSA Labratories' CryptoBytes*, volume 2, 1996.

[154] M. Bellare, R Canetti, and H. Krawczky. Rfc 2104 - hmac: Keyed-hashing for message authentication. http://www.faqs.org/rfcs/rfc2104.html, February 1997.

[155] Matt Bishop. *Computer Security.* Addison-Wesley, August 2003.

[156] Bart Preneel and Paul C. van Oorschot. On the Security of Iterated Message Authentication Codes. In *IEEE Transactions on Information Theory*, pages 188–199, 1999.

[157] Ian Avrum Goldberg. *A Pseudonymous Communications Infrastructure for the Internet.* PhD thesis, University of California at Berkeley, 2000.

[158] B. Schneider. Authentication - Lamport's One-Time Password Scheme. http://www.cs.cornell.edu/courses/cs513/2004sp/NL11Lamport.html, 2004.

[159] A. Perrig, D. Song, R. Canetti, J. D. Tygar, and B. Briscoe. Request for comments 4082: Timed efficient stream loss-tolerant authentication (tesla): Multicast source authentication transform introduction. electronically, June 2005.

[160] Adrian Perring, Ran Canetti, Dawn Song, and J. D. Tygar. Efficient and secure source authentication for multicast. In *Proceedings of the Internet Society Network and Distributed System Security Symposium (NDSS 2001)*, pages 35–46, 2001.

[161] W3C. Web services description language (wsdl) version 2.0 part 1: Core language. http://www.w3.org/TR/wsdl20/, June 2007.

[162] Joachim Zeiss and Oliver Jorns. Context-Based Privacy Protection for Location-Based Mobile Services using Pseudonyms. In *The 2nd International Workshop on Privacy-Aware Location-based Mobile Services (PALMS), In conjunction with the 9th International Conference on Mobile Data Management (MDM'08)*, 2008.

[163] Michael Burrows, Martin Abadi, and Roger Needham. A Logic of Authentication. In *ACM Transactions on Computer Systems (TOCS)*, pages 18–36, February 1990.

[164] Oliver Jorns, Sandford Bessler, and Rudolf Pailer. An Efficient Mechanism to Ensure Location Privacy in Telecom Service Applications. In *International Conference on Network Control and Engineering, Net-Con'2004*, Palma de Mallorca, Spain, November 2004.

[165] Oliver Jorns and Gerald Quirchmayr. Transaction Pseudonyms in Mobile Environments. In *Journal in Computer Virology, Springer Paris*, 2007.

[166] Sun's Java 2 Micro Edition Platform, http://java.sun.com/javame/index.jsp (last viewed 2. October 2008).

[167] Sun's Java Wireless Toolkit 2.5.2 for CLDC,
URL: http://java.sun.com/products/sjwtoolkit/download.html?feed=JSC (last visited 25. September 2008).

[168] Java User Group, MIDP Benchmark, URL: http://www.club-java.com/TastePhone/J2ME/MIDP_Benchmark.jsp (last visited 25. October 2008).

[169] Optimizing for Speed in J2ME, Extreme Tips for Lightning-Fast MIDlets, URL: http://j2medevcorner.wordpress.com/2007/03/13/optimizing-for-speed-in-j2me-extreme-tips-for-lightning-fast-midlets/ (last visited 25. September 2008).

[170] W. Diffie and M. E. Hellman. New Directions in Cryptography. In *IEEE Trans. Inform. Theory IT-22*, volume 22(6), pages 664–654, November 1976.

[171] Chris Alexander and Ian Goldberg. Improved User Authentication in Off-The-Record Messaging. In *Proceedings of the 2007 ACM Workshop on Privacy in the Electronic Society, WPES 2007, Alexandria, VA, USA*, pages 41–47, October, 29 2007.

[172] Audun Jøsang and Simon Pope. User Centric Identity Management. In *Proceedings of the Asia Pacific Information Technology Security Conference, AusCERT'05*, 2005.

[173] Audun Jøsang, John Fabre, Brian Hay, James Dalziel, and Simon Pope. Trust Requirements in Identity Management. In *Proceedings of the 2005 Australasian workshop on Grid computing and e-research*, volume 44, pages 99–108, 2005.

[174] Doug Lea. *Concurrent Programming in Java, Design Principles and Patterns*. Addison-Wesley, 2000.

[175] Rias A. Sherzad. Singleton Pattern in Java, URL: http://www.theserverside.de/singleton-pattern-in-java/ (last visited 2. November 2008).

[176] Erwin Aitenbichler. Development Tools for Mundo Smart Environments. In *Workshop on Software Engineering Challenges for Ubiquitous Computing*, Lancaster University, 2006.

[177] D. Crockford. The application/json Media Type for JavaScript Object Notation (JSON). RFC 4627, URL: http://www.ietf.org/rfc/rfc4627.txt (last visited 21. February 2009), July 2006.

[178] Oliver Jorns and Joachim Zeiss. Using Semantic Reasoning and Privacy Policies in Ubiquitous Environments. In *First International Workshop on Security for Spontaneous Interaction, IWSSI 2007, Innsbruck, Austria*, 2007.

"Ich habe mich bemüht, sämtliche Inhaber der Bildrechte ausfindig zu machen und ihre Zustimmung zur Verwendung der Bilder in dieser Arbeit eingeholt. Sollte dennoch eine Urheberrechtsverletzung bekannt werden, ersuche ich um Meldung bei mir."

Curriculum Vitae

Education

Ph.D. studies in Computer Science
University of Vienna, Austria

Thesis: Privacy in Location-Based Services
Advisors: Gerald Quirchmayr, Erich Schikuta

MSc Computer Science
Vienna University of Technology, Austria

Thesis:
Aspekte der IT-Security als technisches Gestaltungsziel aus Perspektive der Organisation
Advisor: Wolfgang Slany

Professional Experience

Ferdinand Porsche University of Applied Sciences http://www.fernfh.at **since 2009**
Head of study path Business Informatics

ftw. Telecommunication Research Center Vienna: http://www.ftw.at **2002 - 2008**
Researcher

Wifi Vienna: http://www.wifi.eu/EN/eu/default_eu.aspx **1999 - 2001**
Trainer for courses: Web Design (HTML, JavaScript), Java, Java Script

Austrian Science Fund: http://www.fwf.ac.at/en/index.asp **1999**
Web Support

Vienna Input Output System (ViPIOS): Research Project P11006-MAT **1996 - 1998**

Kapsch AG: http://www.kapsch.at/index_en.htm **1991 - 1994**
Technical documentation

Publications

Book (in German)

1. Oliver Jorns, IT-Security Management: Grundlagen, Instrumente, Perspektiven, VDM Verlag Dr. Müller; Auflage: 1 (Oktober 2006), ISBN 3-86550-724-7

Patent (in German)

2. Oliver Jorns, Sandford Bessler, Rudolf Pailer: Verfahren zum Umwandeln von Target-Ortsinfor-mation in Mehrwertinformation Östereichisches Patentamt, Austria: Patent Nr. A 363/2004, Submission Date: 1.11.2004

Book Section

3. Oliver Jorns, Gerald Quirchmayr: A Privacy Enhancing Mechanism for Mobile Tickets using Telecommunication Services, In Applied Information Technology Research - Articles by Cooperative Science Network, University of Lapland, Department of Research Methodology Reports, Essays and Working Papers, Juha Lindfors (ed.), ISBN 952-484-046-4, ISSN 1796-4474, Rovaniemi, Finland, 2007

Journals

4. Jürgen Mangler, Oliver Jorns, Erich Schikuta, Helmut Wanek, Ul Haq: Mobile gSET, Secure, Business Workflows for Mobile Grid Clients, In: *Journal in Concurrency and Computation: Practice and Experience*, John Wiley & Sons, Ltd., 2009

5. Oliver Jorns, Oliver Jung, Gerald Quirchmayr: Transaction Pseudonyms in Mobile Environments, In: *Journal in Computer Virology*, Springer Paris, 2007

6. Thomas Fürle, Oliver Jorns, Erich Schikuta, and Helmut Wanek: Meta-ViPIOS: Harness distributed I/O resources with ViPIOS, In *Iberoamerican Journal of Research Computing and Systems*, Special Issue on Parallel Computing, 2000

Conference Contributions

7. Oliver Jorns, Gerald Quirchmayr. A Middleware for Location-Based Mobile Applications, 10^{th} *International Conference on Information Integration and Web-based Applications & Services* (iiWAS2008), November 24.-26. 2008, Linz, Austria

8. Anna V. Zhdanova, Marcin Davies, Oliver Jorns, Vera Stavroulaki, Panagiotis Demestichas, Marta Gonzalez, Klaus Moessner, Francois Carrez, Hariharan Rajasekaran and Luigi Lo Iacono. MOSS: Mobile Social Spaces, OneSpace 2008 - *First International Workshop on Blending Physical and Digital Spaces on the Internet*, Austria, 28 September, 2008

9. Oliver Jorns, Gerald Quirchmayr. Cross Domain Privacy Protection for Location-Based Services, 14^{th} *Americas Conference on Information Systems* (AMCIS 2008), Toronto, Canada, 14.-17. August, 2008

10. Joachim Zeiss, Oliver Jorns. Context-Based Privacy Protection for Location-Based Mobile Services using Pseudonyms, The 2^{nd} *International Workshop on Privacy-Aware Location-based Mobile Services* (PALMS), In conjunction with the 9^{th} *International Conference on Mobile Data Management* (MDM'08), April 27, 2008, Beijing, China

11. Oliver Jorns, Gerald Quirchmayr. A Transport Ticket System with Location and Privacy Protection, 6th Eastern Europe e—Gov Days, April 23-25, 2008, Prague, CZ

12. Oliver Jorns, Oliver Jung, Gerald Quirchmayr. A Platform for the Development of Location-Based Mobile Applications with Privacy Protection, The 3^{rd} *International Conference on COMmunication System softWAre and MiddlewaRE* (COMSWARE 2008), Bangalore, India, January 6-10, 2008

13. Bernhard Riedl, Oliver Jorns. Granting access to Emergency Data in a pseudonymized e-Health Architecture, 9^{th} *International Conference on Information Integration and Web-based Application & Services*, December 3-5, 2007, Jakarta, Indonesia

14. Ul Haq, Erich Schikuta, Jürgen Mangler, Helmut Wanek, Oliver Jorns. A Gridified, Secure, Mobile Business Workflow Using gSET, *Workshop on Economic Models and Algorithms for Grid Systems* (EMAGS 2007), in conjunction with 8^{th} *IEEE/ACM International Conference on Grid Computing* (GRID 2007), Austin, Texas, USA, September 19-21, 2007

15. Oliver Jorns, Joachim Zeiss. Using Semantic Reasoning and Privacy Policies in Ubiquitous Environments, First *International Workshop on Security for Spontaneous Interaction* (IWSSI 2007), Innsbruck, Austria, 16^{th} September 2007

16. Oliver Jorns, Gerald Quirchmayr, Oliver Jung. A Privacy Enhancing Service Architecture for Ticket-based Mobile Applications, 2^{nd} *International Conference on Availability, Reliability and Security* (ARES 2007 The International Dependability Conference), Vienna, Austria, April 10-13, 2007

17. Oliver Jorns, Gerald Quirchmayr, Oliver Jung. A Privacy Enhancing Mechanism based on Pseudonyms for Identity Protection in Location-Based Services. *Australasian Information Security Workshop (Privacy Enhancing Technologies)* AISW-PET2007 *at the Australasian Computer Science Conference in Ballerat*, Victoria, 30 January - 2 February 2007

18. Barbara Emmert, Oliver Jorns. Prepaid Peer-to-Peer Services: 6^{th} *IEEE International Conference on Peer-to-Peer Computing*, Cambridge, UK, September, 2006.

19. Peter Fröhlich, Oliver Jorns, Raimund Schatz: Considering Context in Mobile Ticketing, International *Workshop on Context in Mobile HCI*, in conjunction with MobileHCI'05, Salzburg, Austria, September 19, 2005

20. Oliver Jorns, Oliver Jung, Julia Gross, Sandford Besser: A Privacy Enhancement Mechanism for Location Based Service Architectures using Transaction Pseudonyms, *Second International Conference on Trust, Privacy, and Security in Digital Business*, (TrustBus'05), Copenhagen, Denmark, August 22-26, 2005

21. Sandford Besser, Oliver Jorns: A Privacy Enhanced Service Architecture for Mobile Users, *Second IEEE International Workshop on Pervasive Computing and Communication Security* held in conjunction with IEEE PerCom 2005, 8 March 2005, Kauai island, Hawaii, USA, 2005

22. Oliver Jorns, Sandford Bessler: PRIVES: A privacy enhanced location based scheme, In *Workshop Proceedings of* 6^{th} *International Conference on Human Computer Interaction with Mobile Devices and Services*, Glasgow, September 13 - 16, 2004

23. Oliver Jorns, Sandford Bessler and Rudolf Pailer: An efficient mechanism to ensure location privacy in telecom service applications, In *Proceedings of International Conference on Network Control and Engineering*, Palma de Mallorca, Spain, November 3 - 5, 2004

24. Lynne Baillie and Oliver Jorns: The Human Interface in Mobile Applications, In 5^{th} *International Symposium on Human Computer Interaction with Mobile Devices and Services*, Italy, Udine, 2003

Given Lectures

- Privacy in Location-Based Services, Intensive Programme on Information and Communication Security, IPICS 2009, 27. - 7. August 2009, Vienna
- TWT1 Technologiesche Grundlagen der Telekommunikationsanwendungen, (Ferdinand Porsche University of applied sciences), Summer 2009
- Lecture at The University of Applied Sciences Technikum Wien, (University of Applied Sciences Technikum Wien), Winter 2008
- 050022/7 PR PI.PRG.EF.PR Einführung in die Programmierung in C++, (University of Vienna), Winter 2008
- 050022 PR PI.PRG.EF.PR Einführung in die Programmierung in C++, (University of Vienna), Winter 2007
- 050031 PI.PRG.EF.PR Einführung in die Programmierung, (University of Vienna), Winter 2006
- 406342 VO+PR WI(Mag)/ISM Information System Security Management, (University of Vienna), Summer 2006
- 050031 AU Einführung in das Programmieren, (University of Vienna), Winter 2005
- 406342 VO+PR WI(Mag)/ISM Information System Security Management, (University of Vienna), Summer 2005
- 401273 AU Einführung in das Programmieren, (University of Vienna), Winter 2004
- 406342 VO+PR WI(Mag)/ISM Information System Security Management, (University of Vienna), Summer 2004

Visited Courses

How (Not) to Write a Research Proposal: Advanced Skills for Successful Proposal Writing, 27.11.2008, Erich Prem, www.eutema.com