Enabling Privacy of Real-Life LBS

A Platform for Flexible Mobile Service Provisioning

Jan Zibuschka, Lothar Fritsch, Mike Radmacher, Tobias Scherner,
and Kai Rannenberg
Johann Wolfgang Goethe University Frankfurt*
Chair for Mobile Commerce & Multilateral Security
Gräfstraße 78, D-60054 Frankfurt am Main, Germany
{zibuschka, fritsch, radmacher, scherner, rannenberg}@m-lehrstuhl.de
www.whatismobile.de

Abstract. Privacy in computerized environments is perceived very differently depending on the respective point of view. Often "privacy enhancing technologies" – initiated by the user, as a measure of self-defense – are seen as conflicting with business goals such as cost-efficiency, revenue assurance, and options for further business development based on existing data. This paper presents the design and implementation of an architecture and prototype for privacy-friendly, interoperable location-based services (LBS), based on intermediation of location data via a location middleware component. The aim is to combine privacy-friendliness, efficiency, and market potential. Therefore the security interests of the stakeholders are analyzed and an architecture solution including an intermediary is introduced. Then the prototype implementation (at a mobile operator) is described and the usage of the prototype for a commercial service and product offer by the operator involved in the development is discussed.

1 Introduction

The high market penetration [1] reached by mobile phones makes these devices a highly attractive platform for the rendering of location-based services (LBS) reaching a broad user base. The mobile operator may provide the location data for specialized LBS providers or act as service provider itself.

However, location data is very sensitive. In many countries and regions there are

* This work was supported by the European Union IST PRIME project; however, it represents the view of the authors only.

even legal requirements associated with the handling of customer data for such purposes. Typically, a mobile network operator is required to obtain permission of its customers before transmitting location information – or, more general, personal information. Also, other privacy laws and regulations, which are varying from country to country and sometimes over time, have to be taken into account. This may lead to unclear or globally inhomogeneous requirements towards the provider of a given service.

So, while mobile operators are − from a technical point of view − in a very good position to supply user location data, the actual provision of location-based services can in some cases be a legal and commercial risk. Thus, there is an incentive to outsource the rendering of location-based services to third parties under clear conditions and to ease the possibility for users to make decisions on the transfer of data. With this strategy, the operator can maintain good and trustful customer relations and get rid of potential liabilities that may arise from the specifics of a service.

However, to be widely accepted, such a system needs to be based on technology available to a broad user base. As it is highly unlikely that the system could be built to be oblivious of underlying technologies (such as WAP 1.x, 2.x, or direct TCP/IP connections) without impeding privacy guarantees, several trade-offs have to be considered during the design of the system.

This paper reports on the design of a system and architecture that try to conciliate stakeholders' interests. Section 2 presents the involved entities and their requirements; section 3 gives an overview of the architecture, followed by the presentation of implementation details in Section 4. Section 5 discusses related work and key benefits, after which section 6 wraps up.

2 Interests and Related Security Requirements

Location-based services are employed for a wide range of use cases. One widely used application are navigation services, e.g. finding the nearest pharmacy and directing the user there. Typically users open a connection to a service via their mobile phones, and then the user's position is determined by the mobile operator. The determined position is passed on to the service provider, who compares it to his database. The results – e.g. the 5 nearest pharmacies – are then returned to the user's mobile phone, where they are displayed.

So the mobile operator usually knows what kind of service the user has accessed, while the LBS provider would be able to tell which mobile operator the user is using. The service then needs to be customized for usage with a specific mobile operator's location provision interface. Additionally, precautions need to be taken to avoid that LBS providers can track users simply at their discretion. By this LBS demonstrate the also more general need for solutions that empower users to enforce privacy policies for their personal data, including their location data. Also LBS are examples of complex services that are offered by consortia; so more than just the two "classic" stakeholders (customer, provider) are involved.

For analyzing the requirements of the different stakeholders involved in the provisioning of location-based services, the concept of Multilateral Security [2, 3] was used. Multilateral Security aims at a balance between the (maybe competing)

security requirements of different stakeholders, which includes considering all involved entities as potential attackers. This is especially important for communication systems, as one cannot expect the various stakeholders to completely trust each other.
The "ideal" of Multilateral Security can be described as follows (see Figure 1):

1. Considering Conflicts:
    a. Different parties involved in a system may have different, perhaps conflicting interests and security goals.
2. Respecting Interests:
    a. Parties can specify their own interests and security goals.
    b. Conflicts can be recognized and negotiated.
    c. Negotiated results can be reliably enforced.
3. Supporting Sovereignty:
    a. Each party is only minimally required to place trust in the honesty of others.
    b. Each party is only minimally required to place trust in the technology of others.

Multilateral Security in general refers to all "classical" security goals, i.e. confidentiality, integrity, availability, or accountability can be in the interest of one party, but not necessarily in that of another. However a typical conflict occurs between the wish for privacy and the interest in cooperation. On one hand parties wish to protect their own sphere, information, and assets, on the other hand they strive for cooperation and wish to establish trust with partners, access services, transfer values, or enable enforcement of agreements.

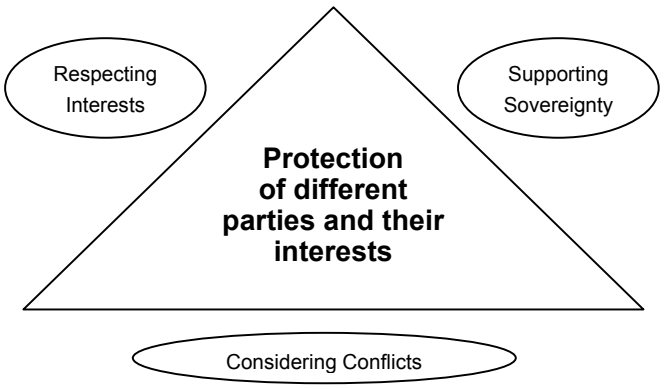

Figure 1: Multilateral Security

2.1 The Stakeholders

The investigation of the pharmacy search scenario leads on first hand to the identification of three different stakeholders:

1. A mobile operator is the owner of the mobile network infrastructure. Its business is to offer the network infrastructure that mobile subscribers use every day, including roaming between different mobile networks. Concerning the provision of location-based services, the mobile operator is often the source for the location information used, and therefore is legally responsible for the release and transfer of the respective data.
2. A service provider is offering LBSs based on the mobile network infrastructure. Classical examples are navigation and routing services such as the pharmacy search scenario illustrated earlier in this section.
3. Last but not least, the users or subscribers of the services have interests. They are often "double" customers: A subscription with the mobile operator enables them to communicate and be mobile, while for specific services they subscribe to the respective specialist service providers.

Detailed analysis of the services and their setting from the different view points and interests yields several requirements for the various entities that will be described in the sections 2.2 till 2.4.

2.2 Mobile Operators' Interests and Requirements

There are mainly five interests from the point of view of the mobile operator:

1. Legal compliance: The mobile operator requires that the interface he provides is compliant with (potentially divergent) privacy legislation.
2. Sovereignty over payment processes: The mobile operator may want to be the entity responsible for the billing of services, even when rendered externally, as this is part of the customer relation.
3. Flexible business models: As different telecommunications markets favour different organizational structures, an architecture supporting mobile operators (MOs), Mobile Virtual Network Operators (MVNOs) or independent parties as location sources is essential for international deployment of the architecture.
4. Customer loyalty: The mobile operator values customer loyalty, which may be increased by respecting each customer's privacy.
5. Standardized communication interfaces: Offering standardized interfaces can enable the mobile operator to offer a wide range of externally rendered location-based services to its users.

2.3 Service Providers' Interests and Requirements

The service provider's requirements focus on his business interests towards user and mobile operator:

1. Standardized communication interfaces: A standardized interface available at the different location sources offers flexibility and limits deployment costs.

2. Trusted payment partners: The service provider requires correct billing for service usage. This requirement also holds for the other stakeholders.

2.4 Users' Interests and Requirements

Users are the weakest of all the parties mentioned, especially if they are acting on their own. So their requirements concentrate on keeping and getting control over their data:

1. Stay anonymous: Users do not want to reveal their identity unnecessarily.
2. Being able to protect the data on one's interests: Users don't want other parties to unnecessarily know what interests they have, e.g. what services they use.
3. Sovereignty over location information: Users require facilities to configure the acceptable usage for their location information.
4. Fine-granular management of consent: Users may want to configure specific parameters concerning the handling of their personal information by different LBS providers.
5. Easy-to-use technology: Privacy functions should not impede usability, especially not the usability of mobile services, as those services are usually used in settings where users cannot simply concentrate on dealing with the user interfaces.
6. Reliable service provision: Availability of the service is a major concern, especially in critical scenarios such as search and navigate scenarios that are used to save time.
7. Confidentiality of service utilization towards mobile operator: A user's service usage patterns should not be obvious for the mobile operator, as it may involve data privileged to the user and the application service provider, e.g. for medical services.

3 Architecture

The stakeholder interests and requirements lead to several architectural requirements. First there are requirements on the controls of the information flows. These are mainly triggered by the users' privacy interests and the interests of the operators and service providers to stay legal:

- To ascertain the proper handling of personal user information by different parties, the system needs to offer a facility for managing user defined (location) privacy policies.
- In addition to enforcing users' privacy preferences, the system should aim to minimize the distribution of information regardless of the users' configured parameters. E.g., it should not be inherently necessary for the mobile operator to know which services a respective user subscribes to.
- Identity management components are needed to make sure that the flow of identity information can be controlled and still services can be accessed by users.

Figure 2 presents a UML use case diagram illustrating the basic components of the system and stakeholder interaction.

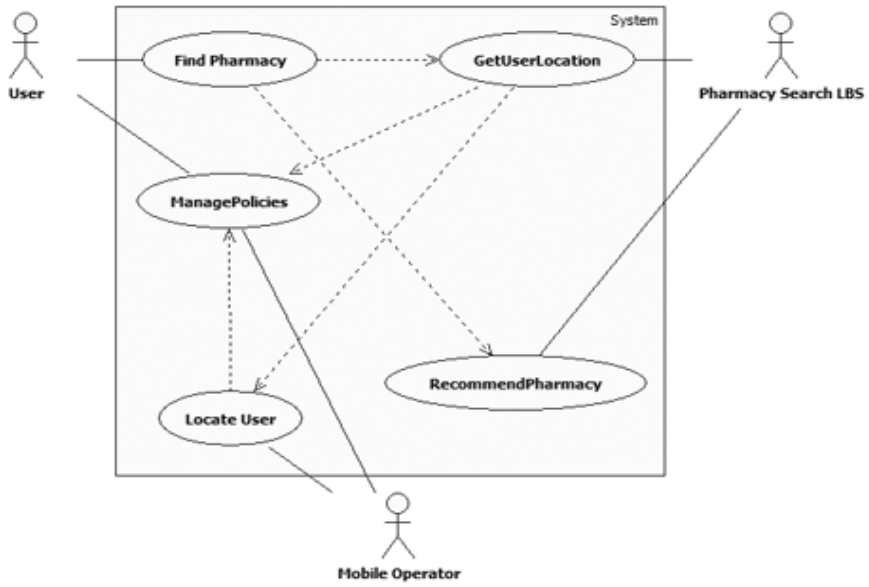

Figure 2: Pharmacy search use case diagram.

To accommodate the operator's and service provider's interests in a large customer base in the mobile market, a compromise between large scale availability of platforms and privacy requirements is needed. On the one hand, the WAP specifications do not allow end-to-end encryption and could be intercepted at the WAP-gateway, which is normally under the control of the mobile operator. Also WAP is sometimes seen as some kind of old-fashioned. However on the other hand, WAP is robust and has a high market penetration, as most mobile phones support this standard and can enable a lot of users to get into the situation of considering and defining their policies.

In addition to having a "stronger" terminal device in a later prototype and a migration path towards the use of this prototype a location middleware component for dealing with weaker devices in a flexible way was designed. The location intermediary is responsible for:

- Providing a policy management front end for clients with limited capabilities (e.g. WAP phones)
- Keeping an audit trail and so empowering subscribers to trace interactions with certain service providers
- Offering anonymization and confidentiality of service usage by providing a proxy between mobile operator and service providers

Mediating the communication between the different stakeholders, an intermediary offers anonymization of relayed traffic, if it is not deployed on the user's device and if some trust can be placed in the entity operating the intermediary (as the traffic is not anonymized against the intermediary). This can act as a fallback solution in cases where the implementation of more elaborate measures (e.g. mixes) is impractical, for example because of restricted client hardware or infrastructure capabilities. However, this will only offer meaningful security guarantees if the connections cannot be eavesdropped at the intermediary by one of the communicating stakeholders. If anonymous communication is available, the intermediary may serve as a rendezvous point for communicating entities [4]. Advanced cryptographic protocols like oblivious transfer have been proposed [5] for the privacy-friendly rendering of location-based services. However, finding a mechanism that minimizes transferred information in the case of bandwidth efficient push services is an open research question.

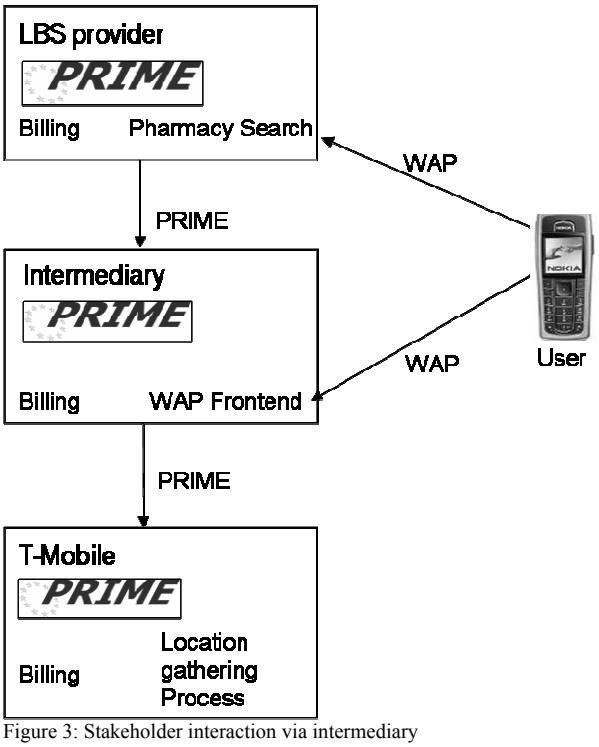

Figure 3: Stakeholder interaction via intermediary

4 Implementation

The implemented example application prototype is a mobile pharmacy search using Wireless Application Protocol l (see Figure 4). The usage of this widely deployed protocol enables the mobile operator to reach a maximum customer base for

upcoming privacy-enhanced products based on the prototype. As it is based on a WAP infrastructure, the prototype does not offer anonymization support.

Figure 4: The pharmacy search application

When a user initiates communications with a service, he is pseudonymized and a communication channel to the MO is established, using the intermediary as a proxy. The relevant privacy policies are checked, and the service can then be rendered. The steps in detail (see Figure 5):

- The user contacts the location-based service provider
- The LBS provider requests an access handle for the current global user pseudonym (e.g. IP address, in the case of no anonymous communication infrastructure) via the location intermediary.
- The LBS provider requests user location and payment allocation from the mobile operator. Policies are managed at the location intermediary in the WAP scenario. The mobile operator may then provide user location and a payment handle to the service provider via the intermediary, if a matching policy is available. If no such policy can be found, the system proposes a policy to the user, based on the service's requirements.
- The LBS provider queries his domain logic, runs the service and provides the result to the user.
- Payment is committed at the mobile operator, again using the intermediary as a pseudonymization proxy.

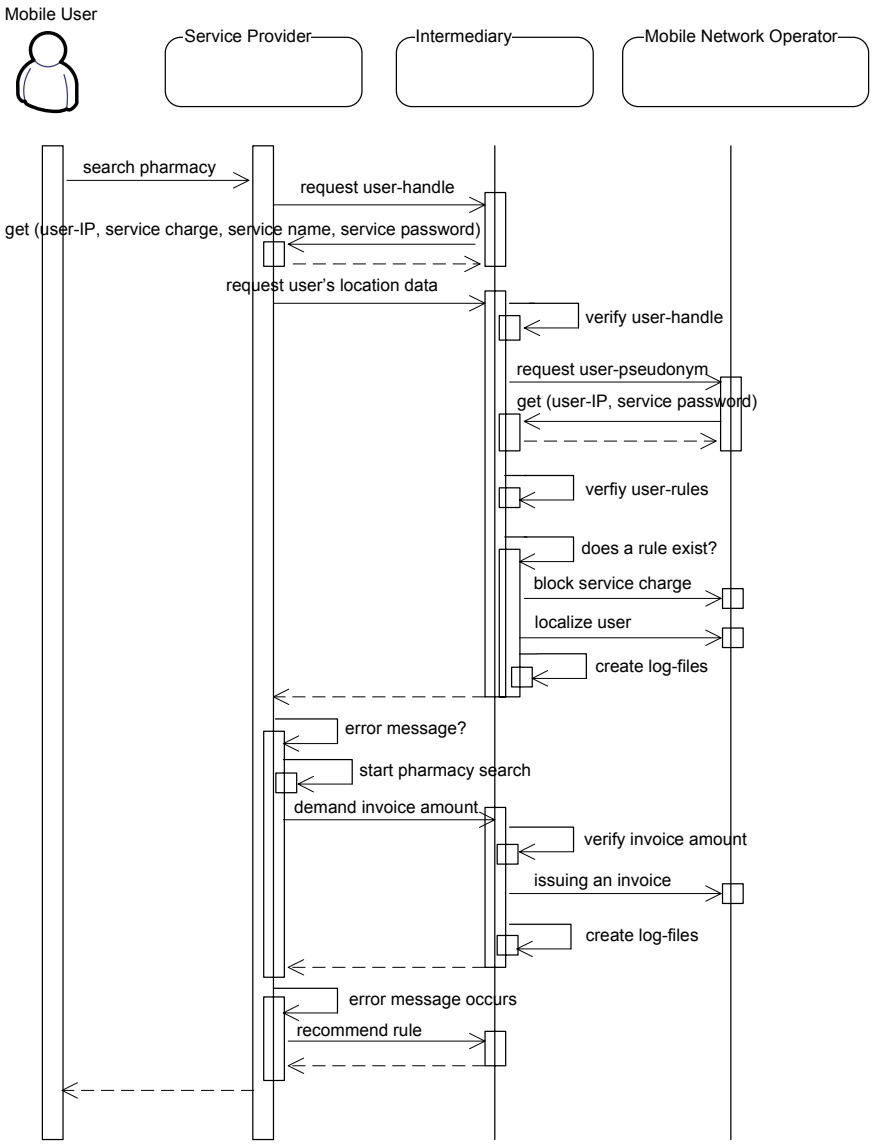

Figure 5: Pharmacy search sequence.

5 Related Work and Key Benefits

There are a wide range of technologies for protecting users' privacy in existence today, which are generally referred to as Privacy Enhancing Technologies or PETs [6]. Several protocols and architectures for the privacy-preserving handling of location information have been proposed. This section gives a quick overview of existing solutions and compares them to the implementation presented in this paper.

The Alipes platform [7] offers the possibility to control the access to location information using user-configurable privacy policies. Furthermore, location information from different sources may be aggregated. However, Alipes does not offer pseudonymization functionalities, and generally no further identity management functionality.

In [8], a system that limits the accuracy of handed-out location information based on the recipient is proposed. However, neither access control functionalities nor pseudonymization are considered.

The architecture presented in [9] proposes pseudonymization and access control functionalities for the location-based services scenario. However, no further analysis of the information flow between the communicating entities is performed.

The intermediary architecture offers several key advantages, corresponding to the requirements raised in section.

- *Interoperability:* An intermediary provides a standardized interface for LBS providers, allowing them to access location data in a unified way. This mediation of location information would then allow tapping the network effect immanent in the distributed, multi-party LBS scenario. Mobile operator independence, roaming support, and the unified interface for service providers for easy deployment and migration seem to be viable business propositions in a fast-moving marketplace. Mobility between different services, location sources, involved market players, and applications seems beneficial from users' and service providers' perspective alike. From an ordinary user's point of view, cost effectiveness, synergy effects, and convenient service usage are major issues.
- *Multi-channel strategy:* An intermediary can collect location data from various sources (GSM, WLAN, and GPS) [10].
- *Synergetic location aggregation:* An intermediary can aggregate multi-channel location information for the benefit of higher quality [11].
- *Simplification:* Intermediaries simplify process handling for LBS providers by removing the need to negotiate contracts with various location sources.
- *Cross-Operator applications:* Without an intermediary, the creation of user-to-user LBS with customers using mobile services at distinct mobile operators is much harder.
- *Pricing advantages:* Intermediaries provide many economic benefits in information markets, e.g. an intermediary buys location information from location providers in large amounts, and therefore is in a position to negotiate cheaper prices. For LBS that consume small quantities of location data, it may be cheaper to acquire location from an intermediary than from a location provider. Other benefits of information intermediaries can be found in [12].

There are different deployment scenarios for the intermediary component, reflecting different business models and organizational structures that are employed in the telecommunications industry. It may be deployed directly at the mobile operator, at a MVNO, or outsourced to a completely independent party. This also gives mobile operators the freedom to treat the intermediation of identities as either a core business or as a sideline of the business. In the first case the intermediation will stay close to the mobile operator but other entities providing a comparable intermediary function will be supported, so that the user has choice(even if many users practically don't use it). In the second case the intermediation can simply be outsourced.

6 Summary and Outlook

We presented the design of a privacy-preserving application architecture and a related prototype. The implementation was realized on a limited budget, and to the satisfaction of both project officials and industry partners. It is now being used for the development and implementation of a commercial service and product offer as well as for initialising a roadmap for further privacy enhancing services, including a second version based on a stronger terminal (with Java functionality) and using more powerful communication protocols (e.g. GPRS).

The current prototype served and still serves as a proof of concept for enabling users to manage access to their data. It demonstrated for management, business development and customer relation minded parties that privacy requirements do not need to preclude the realization of services with viable business models. It also showed that new services do not necessarily violate privacy requirements if care is taken to balance the stakeholders' interests, e.g. in the sense of multilateral security.

Further it gives some hints on possible developments in the market: Beyond a deployment of identity management functionalities at user or services side, there is also the possibility of a market dominated by independent intermediaries that chose localization and connection options dynamically from a pool of available possibilities – for example, from several MOs and MVNOs – based on the users' policies and preferences. Thus, dynamic party matching recommendations may be used to leverage network effects, building a market that offers ease-of-development and ease-of-deployment to service providers while preserving users' privacy. A further standardization of such an interface would allow LBS interoperability between operators, offering an additional incentive for service operators' acceptance of location-based services. This raises new requirements for identity management frameworks processing location information, but also presents a promising use case for advanced privacy-preserving features.

Acknowledgments: We would like to thank Georg Kramer, Tobias Koelsch, Marc Wilhelm, Klaus Kehr, and Arne Pöppel from T-Mobile, Pete Bramhall from HP Labs, and all our colleagues in PRIME for their good and fruitful cooperation and their valuable contributions.

References

1. Bundesnetzagentur: Jahresbericht. 2005.
2. K. Rannenberg, “Recent Development in Information Technology Security Evaluation – The Need for Evaluation Criteria for multilateral Security”, in Richard Sizer et al.: Security and Control of Information Technology in Society – Proceedings of the IFIP TC9/WG 9.6 Working Conference August 12-17, St. Petersburg, Russia, North-Holland, Amsterdam, pp. 113-128, 1994.
3. K. Rannenberg, “Multilateral Security - A concept and examples for balanced security”, *in Proceedings of the 9th ACM New Security Paradigms Workshop*, Cork, Ireland: ACM Press, 2000, pp. 151-162.
4. T. Koelsch, L. Fritsch, M. Kohlweiss, D. Kesdogan, „Privacy for Profitable Location Based Services”, *Proceedings of the 2nd Intl. Conference on Security in Pervasive Computing*, Lecture Notes on Computer Science (LNCS 3450, pp.164-179), Springer; Boppard, Germany, 2005.
5. M. Kohlweiss, B. Gedrojc, "Flexible Location Based Service Protocols Using Efficient Oblivious Transfer", *Kryptowochenende*, 2006.
6. G.W. Blarkom; J. Borking; J.G. Olk: Handbook of Privacy and Privacy-Enhancing Technologies. College bescherming persoonsgegevens, The Hague. 2003.
7. K. Synnes; J. North; P. Parnes; Location Privacy in the Alipes Platform; Institutionen för Systemteknik; Lulea University of Technology; 2002.
8. R. Cheng; S. Prabhakar: Using Uncertainty to Provide-Preserving and High-Quality Location-Based Services, in: Workshop on Location Systems, Privacy and Control, 2004.
9. Jorns, O, -Bessler, S.: PRIVES: A privacy enhanced location based scheme, in: Workshop on Location Systems, Privacy and Control, 2004.
10. A. Albers, S. Figge, M. Radmacher, “LOC3 - Architecture Proposal for Efficient Subscriber Localisation in Mobile Commerce Infrastructures”, *in Proceedings of 2nd IEEE International Workshop on Mobile Commerce and Services (WMCS'05)*; München, 2005.
11. T. Lindner, L. Fritsch, K. Plank, K. Rannenberg, „Exploitation of Public and Private WiFi Coverage for New Business Models”, *Proceedings of the 4th IFIP Conference on E-Commerce, E-Business, and E-Government (I3E),* 2004.
12. F. Rose, The economics, concept and design of information intermediaries. Heidelberg, Physica-Verlag, 1999.