Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

Enabling Efficient and Privacy-friendly Location-based Services with Standardized Intermediary Infrastructures

Tobias Scherner
University of Frankfurt

Enabling Efficient and Privacy-friendly Location-based Services with Standardized Intermediary Infrastructures

Tobias Scherner
Chair of Mobile Commerce and Multilateral Security
Johann Wolfgang Goethe University Frankfurt
tobias.scherner@m-lehrstuhl.de

ABSTRACT

This paper describes a possible solution how disaster management systems using mobile networks could serve as a basis for creating a standardized framework for privacy-friendly and worldwide interoperable location-based services. Positive network externalities can be realized by introducing intermediaries into today's Location-based Services (LBS) architecture for achieving a higher degree of technical compatibility. Furthermore, intermediaries can be used for providing legally compliant and privacy-friendly multiparty LBS to mobile subscribers and therefore increase attractiveness of LBS itself.

Keywords

Disaster Management, Trust, Privacy, Interoperability, Intermediary Infrastructures, Roaming

INTRODUCTION

Today's highly sophisticated LBS, such as mobile communities, friend finder applications and mobile marketing are characterized by flexible and dynamic constellations of different business partners who collaborate in offering their services to mobile subscribers. Different services are often provided simultaneously and in a dynamic context, e.g. related to professional and private life, and should not overstrain users in configuring and administrating their services.

The more complex the services become and the more mobile and fixed-line internet converge, the merrier LBS are going to evolve towards communities with an emphasis on mobile aspects such as providing location information to other users (Vascellaro 2007). But even the integration of using multiple information sources, like GPS, Cell-ID and Wifi-based positioning, which are used by different processors, at different times, in different contexts and for different purposes is currently not fully realized. Today's service provision normally finds its final limitation when different mobile operators are involved and fails across national borders.

On the other hand, modern Disaster Management Systems (DMS) for warning, locating and instructing civilians became reality during the last few years (blogger.com 2005). These approaches use existing mobile communication network infrastructures for getting warnings out to the public. Governmental institutions provide most services, like in the Netherlands (blogger.com 2005), which serve the duty to protect the citizens' physical and mental inviolability. These services represent a first link between DMS and commercial LBS.

The agenda of this article is as follows. First, relevant failures of today's LBS are identified. Second, the demand for LBS disaster management is sketched out and an already developed architecture is presented. An Identity Management (IdM)-system for DMS communities (Executive Office of the President of the United States 2005), enhances this architecture for enabling the spectrum of required DMS functionalities. Locking deeply into mobile network-based DMS, this kind of LBS service has a lot in common with commercial LBS. Ensuring reliability and performance of multi-party-communication systems is critical for the acceptance of both kinds of systems in order to avoid faked messages, loss of credibility (160 character association 2006) and performance problems. On the other hand, DMS normally serves only one purpose – warning civilians in the case of disasters, which is costly for governments (blogger.com 2005)and mostly combined with a low probability of occurrence of disasters. Especially, the community characteristics of DMS are an important analogy to highly sophisticated LBS (Vascellaro 2007). Consequently, this is the motivation for enabling profitable commercial LBS by adapting DMS architecture.

Further on, backed by economical theory, the author concludes IdM, technical and economical requirements which a Service Oriented Architecture (SOA) shall fulfill. Based on these stipulated requirements, the existing architecture is adapted and

justified by design decisions. Afterwards the proposal is evaluated against the requirements. Finally, the limitations of the proposed systems are presented before concluding the findings.

WHERE LBS FAILED AND RELATED WORK

Perceived Lack of Transparency, Consent and Trust

Data protection commissioners, like the German data protection commissioner Peter Schaar (Spiegel online 2007), criticize that current systems and data flows are not appropriate for LBS. For example, replying to Short Message Service messages or approaches of a similar nature are not suitable to communicate informed consent for been located. Complex LBS scenarios include data, which is unique for LBS such as location data of different users, communication profiles and personal relationships and does therefore require special protection measures.
Even if communication partners are trusted to handle users' data as expected, it is currently unclear to many users in how far different parties, e.g. the government, may access their data without informing the data subject (Vascellaro 2007).
The resulting lack of trust is not a new phenomenon and is not unique for LBS (Hoffmann et al.1999). That privacy is a special issue in the context of LBS is underpinned by O'Connor and Godar (2003). Barkuus (2004) showed that users discontinue having the same level of concern when they are using LBS. Therefore, to the author argues that the perceived trust before using LBS for the first time is important for the actual acceptance of services and establishments of global services (Backhouse et al. 2005).
Signaling privacy-protection by industries' self-regulation might help building trust (Moores and Dhillon 2003). However, the LBS industry has not found a common approach for self-regulation. Some related work (Rice et al. 2004), bases on the assumption, that customers would be willing to supply their personal data to companies if they got a fair compensation (Culnan and Armstrong 1999). That implies that users still stay in control of the flow of their data. Koelsch et al. (2005) proposed an intermediary infrastructure for guarding and enforcing users' privacy and offering profitable LBS to service providers

Lack of Established Technical Standards

Current Location-based services suffer from a low degree of compatibility of different services. One can further distinguish between incompatibility of infrastructures along the value chain (vertical incompatibility) and incompatibility of different (initially interdependent) value chains (horizontal incompatibility).
The first problem area can for example be illustrated by the lack of commonly agreed location formats in business processes. So far, different formats of location data are used, but no format has been established as a de facto standard. One of the most popular formats is WGS-84 ellipsoid (National Geospatial-Intelligence Agency 2000), which represents the geodetic basis of the Global Positioning System (GPS) and serves as the standard for aviation. Even the countries of the European Union have not been able to agree on a certain geodetic basis (Voser 2000).

The second problem is the interoperability of different instances of initially independent value chains and offering the possibility of including several service providers into one service delivery. For example, most community services have to rely on compatibility of service delivery provided by different mobile operators and service providers for enabling services like friend finder or child watch. These value-adding networks do not work properly or do not work at all in most cases so far. Economides (1996) analyzed how positive network externalities could be realized and concludes that it is not simply a matter of compatibility of links and nodes of different networks. He points out that "links in networks are potentially complementary but it is compatibility that makes complementary actual (Economides 1996)".

For ensuring interoperability among different networks and countries, standardization bodies like the European Telecommunications Institute (ETSI) started to define and establish standards for communication during emergency cases between different concerned communication partners. These standards may become an important step towards harmonizing privacy-sensitive communication and serve as a basis for commercial Location-Based Services. The MESA Project, a partnership between ETSI and the Telecommunications Industry Association (TIA) has recently published a document (ETSI 2006) summarizing requirements related to disaster management topics with explicitly mentioning commercial secondary use of infrastructures for public safety.

DEMAND FOR MOBILE NETWORK-BASED DISASTER MANAGEMENT SYSTEMS

During the last decades, the frequency and amount of lost, injured and killed people, caused by disasters have grown rapidly (Munich Re Group 2006).

Kron and Thumerer (2002) showed that public authorities as well as potentially affected people have to be involved in preparedness measures. According to Turoff et al. (2006) the necessity of being used to a system also applies to citizen level.

Additionally, warning infrastructures that are only used for these purposes often become outdated, un-maintained and do not get adapted to changing requirements (Gruntfest and Huber 1989).

The Munich Re group (2002) investigated elements of best practice procedures of company internal communication for limiting affects of disasters. The author concludes that reliability, honesty, clarity, responsibility, speed and accessibility to information are key features of warning systems, similar to other LBS. Therefore, the author concludes that a lack of information distribution tends to lead to distrust, rumors and panic. A concept for ensuring integrity and authenticity of public broadcast warnings is described in Roßnagel and Scherner (2006).

Related Work in the Area of Disaster Management

As described in Fritsch and Scherner (2005) and Scherner and Fritsch (2005), mobile network-based warning systems, as special LBS, are useful for saving lives in emergency cases and might contribute to reducing damages and loss, depending on the kind of disaster. This work focuses on the research question of how, during large-scaled disasters, issued warnings could satisfy the following features:

- Warning civilians before and, as far as possible, assist after the occurrence of disasters.
- Supporting regular rescue forces by pre-registered and verified specialists (medics, firefighters, etc.).
- Notifying contact persons about the whereabouts of victims. This functionality reduces uncertainty of whereabouts and requires automated observation rules.
- Persons who have registered beforehand are notified when emergencies occur to their property.

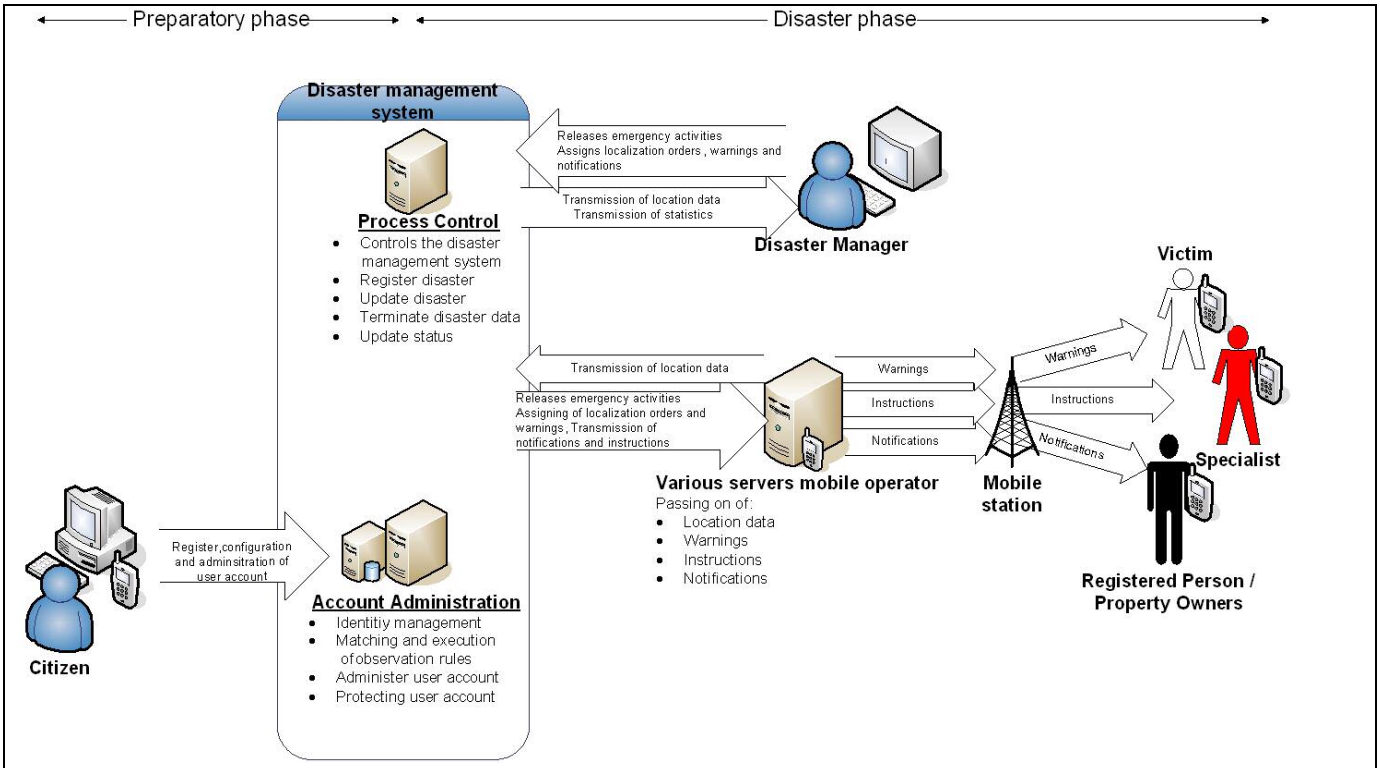

Figure 1: Disaster Management System

Their proposed system provided users anonymity towards the disaster manager and pseudonymity for specialists and observers of next-of-kin and properties (Fritsch and Scherner 2005) and was under the control of governmental authorities. In this system, the disaster manager was the only authority permitted to access personal information. Users were able to trace access to their data via data track functionality. The underlying complexity of the flow of personal data was relatively low. Consequently, assurance that the infrastructure will protect users' privacy was relatively easy to provide compared to multi-party scenarios.

Enhancing the Infrastructure for Multiparty-disaster Management Purposes

Gomez et al. (2006) report that communities of specialists combined with modern information and communication technology (ICT) have a strong impact on preparedness for disasters. In the initially mentioned model, specialists were characterized by some simple certified attributes (e.g. firefighter and car mechanic) in the system. Disaster managers were able to contact required specialists staying nearby the disaster area. This feature allows centralized coordinators to organize the next appropriate steps. However, taking into account that disaster events often result in a high and spontaneous amount of coordination effort in the shortest of times, this approach might become unfeasible.

Turoff et al. (2006) identified a demand of interconnecting organizations and individuals by gaming scenarios. Sheiderman and Preece (2007) found out that social networks, like neighborhoods and other local communities play an important role. Citizens have to be able to form dynamic teams in emergency cases and to participate remotely without direct involvement of centralized disaster managers. Front-line responders for improving effectiveness between agencies may also assist these teams. Furthermore, the participants may have multiple roles in such a community and such roles have to be determined and managed in an identity management system. Consequently, this functionality requires many personal data, which have to be adequately protected.

CONCLUDING REQUIREMENTS FOR LBS

Theoretical Economic Foundation

Evolution of LBS has shown that neither pure market-driven solutions resulted in a prospering LBS market, nor technical regulation initiatives ended with suitable solutions. Burke et al. (2004) showed that mobile operators have not fulfilled the E911 requirements stipulated by the Federal Communications Commission (FCC) in providing locating technologies for emergency cases for a long time. One could conclude that regulating the market of location information in technological means will not successfully take place without respecting the requirements of mobile subscribers and mobile operators.

Katz and Shapiro (1985) have shown, that higher output, and thus in their model, higher service consumption can be realized if firms agree on compatibility. In this case, services have to be compatible and can be used by more users interacting with each other across several mobile operators.

Shapiro and Varian (1998) analyzed generic strategies in network markets for introducing new information technologies. They did their analysis on microeconomic level, which means, that they proposed strategies to companies and alliances and not for whole industry sectors, which is what this article is aiming at. Nevertheless, the lessons learned from the past lead to suggesting a strategy that could satisfy mobile subscribers, mobile operators, service providers and the government:

These four generic strategies are characterized by two different kinds of trade-offs. The first trade-off exists between performance and compatibility, the second one between openness and control. As stipulated before, the aim of this paper is to analyze strategies that allow compatibility of services across several mobile operators. Therefore, the performance strategy is excluded. The next important question is the degree of openness, respective control of mobile operators over interfaces, customer relationships, and therefore their possibility of influencing future development of LBS.

Economides (1996) shows that firms with a high service demand generated by their own customers have an advantage to deviate from an agreed standard if their customers could still use the services of the other firms but not vice versa.
However, declining airtime prices indicate that mobile operators and their service providers might increasingly opt for differentiation strategies characterized by premium services (Figge and Rannenberg 2004).
One can conclude that some degree of compatibility of interfaces is critical for escaping from the current deadlock.
Therefore, a truthfully principal who provides coordination to agents (mobile operators and service providers) might improve the current situation (Weitzel 2003).
A strategy is required, which offers high compatibility and privacy protection while simultaneously offering mobile operators a potential for differentiation. As stated by Grindley (1995), governmental authorities and official standardization bodies tend to concentrate on technical aspects rather than on commercial and strategic issues. Therefore, fearing the force of supranational (governmental) authorities regulating the DMS and thus the LBS infrastructure might enforce de facto standards as a market-determined solution.
For enabling interoperable and efficient LBS, the following IdM, technical and economical requirements have been compiled. The GSM Association (2003) has already documented some of these requirements in its technical report.

IdM Requirements

The above-characterized demand for trust, consent and transparency could be addressed by providing an identity management system to mobile subscribers where they are able to configure and administer the following features:

1. Informed consent administration

   Users need to provide their informed consent to data collection, data processing and data transmission. The system has to empower the user to determine what the consequences of consenting are, who the recipient is, which service is to be used and what the recipient is allowed to do with the data. Furthermore, the system has to provide mechanisms of revoking consent at any time.

2. Notification

   Users have to have the ability to determine notification rules before they are located. The notification frequency may vary between once subscribed to a service and once per location request.

3. Data track functionality

   The IdM-system has to provide data tracks for empowering the users to determine who accessed which data and for what purpose. Satisfying this requirement tends to result in a higher acceptance level of the mobile subscriber towards LBS.

The identity-related requirements are for example subject of research of the PRIME project (PRIME consortium 2007).

Technical Requirements

1. Users consent shall be interoperable across different service providers and mobile operators

   Based on the IdM-requirement no.1, mobile operators have the requirement of operating on a legitimate basis and are able to manage their mobile subscribers consent across different service providers, different mobile operators and across national borders.

2. Integration of different location sources

   Depending on the availability, personal preferences, accuracy and actual cost of location data, the infrastructure shall enable the mobile subscriber to decide which location source should be used, preferably by predefined rules. Some approaches of combining several location sources are published, e.g. by Albers et al. (2005).

3. Smooth integration of services without regulating end-users technology

   End-users should be able to use their already existing equipment for fundamental services. High prices for new equipment tend to result in reduced acceptance thresholds of end-users.

4. Openness

   The infrastructure shall be open for integrating easily new LBS-applications as well as new mobile operators.

Economical Requirements

1. Differentiation potential

   Mobile operators still have potential for differentiation, e.g. by providing premium services.

2. Cost efficient billing procedures

   Charging for LBS should follow standardized clearing procedures in a cost-efficient way, including rollback mechanisms in the case of uncompleted service delivery to end-users. Users should have the opportunity of being billed via their mobile operator.

3. Minimization of maintenance overhead

   Currently, all parties along the value chain have to establish contracts with each business partner they are working with. An important requirement is therefore that mobile operators as well as service providers shall be able to minimize the number of business contracts and the corresponding maintenance overhead of their contractual relationships.

Following the terminology of Economides (1996), the market of mobile-network-based LBS is caught in oligopoly structures under incompatibility, which means that the oligopolists (in this case the mobile operators) are producing incompatible goods (LBS) only for their own customers (mobile subscribers). As long as these deficiencies hold, it seems unlikely that the willingness to either pay for or to use LBS will significantly increase.

PROPOSED NEW INFRASTRUCTURE

Based upon the experiences gained with a DMS-related scenario, an improved infrastructure is proposed, which comprises the following entities and features:

Mobile Operator

The mobile operator offers an IdM-system to mobile subscribers, which allows creation of service policies, corresponding information flow rules, consenting to locating procedures and choosing amongst different available location sources. Occurring events, like access and exchange of personal data have to be logged by data track functionalities. These logs are accessible for the user upon request. The mobile operators still stay in control of their customer relationship and charge the mobile subscriber for consumed LBS.

LBS Intermediary

The intermediary, serving as a principal (Weitzel 2003), takes care of initiation and maintenance of contracts towards mobile operators and service providers. The intermediary is also in charge of negotiating interfaces with mobile operators and service providers. Consequently, the intermediary takes over clearing processes for service providers and mobile operators. Furthermore, the intermediary enforces privacy and identity obligations set by mobile subscribers, which could vary between total anonymity and several degrees of pseudonymity towards the service provider. T-Mobile international for example implemented such a prototype with the focus on privacy protection and first results are promising (Zibuschka et al. 2007).

LBS provider

LBS providers offer their services to mobile subscribers through the LBS intermediary and mobile operators. They have to provide evidence that they comply with the mobile subscribers' predetermined privacy rules and information flows. The LBS provider and LBS intermediary, who have to monitor the compliance, agree bilaterally on the contractual conditions for service provisioning. Particular services, like DMS might have the right to override user defined privacy rules. Nevertheless, this has to be legally compliant, transparent to the user and noted in the data track. In Figure 2, the resulting architecture is introduced.

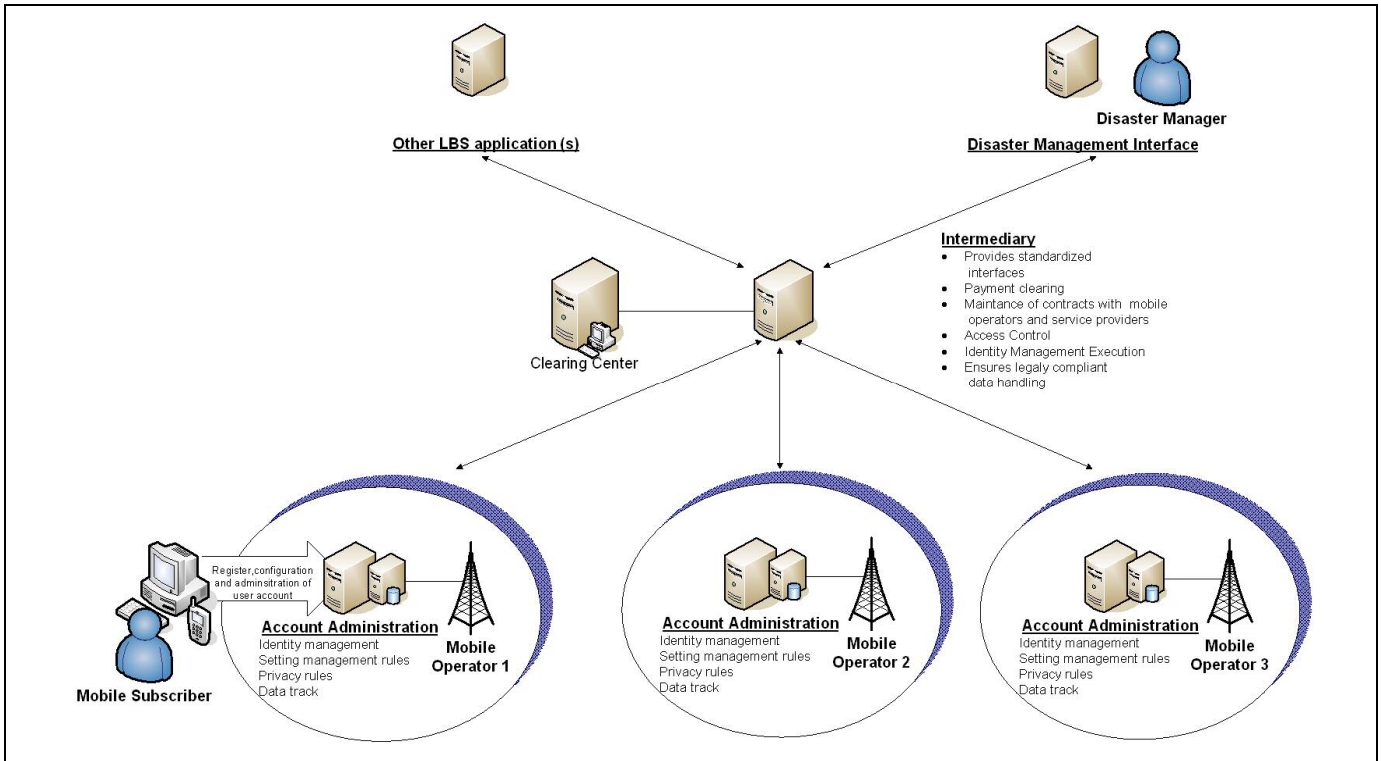

Figure 2: Revised infrastructure

Design decisions

The proposed adjustments of the infrastructure imply changes in the deployment of the initially proposed DMS. The most prominent change relates to the user account administration, which is now deployed at the mobile operator's sphere. The following arguments justify this decision.

Mobile operators want to stay in control and protect their customer relationship, including payment and cash flows

Being a first mover in providing compatible LBS combined with additional premium services can result in a short- or mid-term competitive advantage as described for communities by Hagel and Armstrong (1997). One of the mobile operator's most valuable assets is profitable customer relationships. Therefore, it is possible to conclude that the majority of mobile operators prefer to deploy the account IdM-system under their control. One strong indicator that mobile operators regard users' identity management as a competitive factor is that they can create lock-in effects if the users' data is not easily transferable from one IdM-system to another, even when the interfaces to the intermediary or service provisioning are standardized. Special features of the IdM-system could serve as a unique selling proposition and therefore enhance customers' loyalty. Additionally, mobile operators are able to choose whether they opt for technical leadership, introduce standards products or complementary assets for creating visible benefit of their label to customers. Nevertheless, the most promising strategy seems to join an alliance with one of the upcoming IdM-approaches, like Sxip (Sxip Identity Corporation 2007).

Users' trust in mobile operators vs. users' trust in unknown facilities

The second argument for deploying the mentioned component under the control of mobile operators is closely related to the fuzzy topic "trust" and it is more an educated guess than based on facts. "Trust" has many meanings, and each individual has a different perception. Currently, mobile operators have the full control and could gain access to all LBS-related data anyway. Mobile operators know where their subscribers have been, which transaction they did, for which price and with whom. In most cases, this data is not allowed to be merged without authorization, but it is already under the control of the mobile operator. Therefore, the author concludes that a deployment of the privacy-protecting components in the sphere of the mobile operators would be in favor of most subscribers. In the long term, other IdM-systems might replace proprietary solutions and become more effective when they are combined with other identity management aspects.

Avoiding long-term governmental influence on the market

It seems unlikely that governmental authorities are willing or allowed to run such an infrastructure for commercial services, at least in Europe. Contrariwise, the European Union as well as national regulatory authorities have been anxious to deregulate the telecommunication market and to strengthen free competition among market players in the last decades. Therefore, it is proposed that the intermediary infrastructure is set up as an independent entity, which offers services to communication and service providers. Consequently, communication infrastructures are not narrowed to mobile communication networks but other networks are out of scope of this article.

EVALUATION OF THE PROPOSED INFRASTRUCTURE

For evaluating the compliance of the revised architecture, the stipulated requirements are reviewed in this section.

IdM and privacy functionalities

The proposed infrastructure ensures that users stay in control over who is going to receive which personal data and for which purpose. Fine grained policy-management offers users the ability of defining sets of predefined IdM and privacy rules that will apply to certain services. Users are able to define notification rules on how they would like to be informed that they were located.

All data transferred to LBS providers could be verified by inspecting the data track functionality from time to time. This functionality follows a multi-channel strategy and access via mobile and fixed internet is possible.

Technical requirements

The infrastructure offers mobile operators a legal framework of verifying users' consent by querying his IdM-account as part of their roaming services. This approach also reduces the complexity for mobile subscribers because they could express their consent in their mother language although the service itself is provided in another language.

Integrating users' location source preferences in the IdM-system enables smart service delivery. Mobile operators know the characteristics of the mobile device used, for example, whether it is GPS-enabled, or not. Matching available location sources against requirements of the service at the mobile operator sphere therefore minimizes the flow of potentially sensitive data at a very early stage.

Supporting different location sources enables mobile subscribers to use their already available equipment and offers potential for a large installed base.

Using an LBS intermediary lowers the entrance barrier for new LBS providers, which would otherwise have to contract with each mobile operator individually and offers the chance for widely accepted interfaces.

Economical requirements

The proposed infrastructure introduces with the LBS intermediary a centralized charging and billing activity that is in charge of clearing procedures between different mobile operators and mobile operators and service providers. Mobile operators still have the freedom to contract with LBS providers on a bilateral basis for providing premium services.

The LBS intermediary offers the chance to develop de facto standards for interfaces by negotiating frameworks and maintaining technology with the relevant market players. Furthermore, introducing this entity reduces the overall effort of agreeing and versioning of contractual relationships, which could be delegated to a principal. Such an entity might be a joint venture of mobile operators, similar to examples of the banking sector (Swiss Interbank Clearing 2007).

This solution does not necessarily provide a global maximization of network-wide return on investments. However, it might create better results than the current scenario (Weitzel 2003).

Limitations

Still, users have to be confident that service providers will apply privacy rules as stipulated by the mobile subscriber. Casassa Mont (2006) proposed solutions on how these obligations could be enforced by users remotely, given that the service provider upgrades its infrastructure. Casassa Mont and Crane (2006) have described the required elements of such architecture.

Realization of the proposed infrastructure could be reached by governmental regulation or by consensus among the LBS-industry. Changing licenses of mobile network operators is in the first place not very popular with the industry and is not necessary if governmental authorities and the LBS-industry agree on a standardized approach.

The consensus approach offers mobile operators and service providers the opportunity to discuss how to maximize the expected outcome for all concerned parties. Nevertheless, agreeing on feasible solutions also includes that side payments have to be considered (Weitzel 2003). These side payments do not necessarily have to be paid by the commercial market players themselves. It is a common approach in mobile networks that regulation authorities grant incentives to economically disadvantaged players. For example, the German regulatory authority grants different fees to mobile operators when a call comes in from a different network, which has to be paid by the caller. These fees shall compensate their additional cost due to later market entry and the resulting available higher radio frequency.

CONCLUSION

In this paper it was shown that it is technologically possible to provide efficient and interoperable LBS. Based upon the analysis of requirements, a revised design of the proposed architecture was introduced. This solution has the potential to overcome the current incompatibility dilemma of the LBS industry. One conclusion is that the proposed infrastructure enables cost-efficient business processes while offering potential for differentiation to mobile operators. The introduced intermediary acts as a principal for the LBS-industry. This approach enables multilateral interaction between mobile subscribers across different mobile operators. Furthermore, IdM-features are introduced to LBS without the necessity that users have to configure privacy and identity rules for each used service separately. Additionally, smart integration of new services can be executed easily. However, it is not predictable from the current point of view, whether the market players will agree on a collaborative approach.

References

1. 160 character association News “SMS Alerts A Disaster?“ *http://www.160characters.org/news.php?action=view&nid=1892,* accessed 26-Jan-2007.
2. Albers, A., Figge, S. and Radmacher, M.: LOC3 - Architecture Proposal for Efficient Subscriber Localisation in Mobile Commerce Infrastructures, Proceedings of 2nd IEEE International Workshop on Mobile Commerce and Services *(WMCS'05),* Munich, 2005.
3. Backhouse, J., Hsu, C., Tseng, J. C. and Baptista, J.: A Question of Trust, Communications of the AC (48:9), 2005, pp. 87-91.

4. Barkhuus, L.: Privacy in location-based services: Concern vs. coolness, in G. Iachello, M. Raento and I. E. Smith (Eds.), Mobile HCI 2004 Workshop on Location Systems Privacy and Control, Glasgow, 2004.
5. Burke, K. and Yasinsac, A.: The ramifications of E911, College of Arts and Science, Tallahassee, Florida, USA, 2004.
6. Casassa Mont, M.: On Privacy-aware Information Lifecycle Management in Enterprises: Setting the Context, in ISSE 2006 (Eds.), 10. - 12., Rome, Italy, Oct. 2006.
7. Casassa Mont, M. and Crane, S.: Customizable Privacy Assurance System based on Active Feedback, Hewlett Packard Technical Report, HPL-2006-56, 2006, 15 pages.
8. Culnan, M. J. und Armstrong, P. K.: Information Privacy Concerns Procedural Fairness, and Impersonal Trust: An Empirical Investigation, Organization Science (10:1), 1999, pp. 104-115.
9. Culnan, M. J. How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. MIS Quarterly (17:3), 1993, pp. 341-363.
10. Economides, N.: The Economics of networks, International Journal of Industrial Organization, Volume 14, 1996, pp. 673-699.
11. European Telecommunications Standards Institute (ETSI): Statement of Requirements (SoR) ETSI TS 170 001 V3.2.1, Project MESA Service Specification Group - Services and Applications, Sophia – Antipolis, 2006.
12. Executive Office of the President of the United States / Office of Science and Technology: Grand Challenges for Disaster Reduction: National Science and Technology Council, Washington D.C., 26 pages, http://www.sdr.gov/SDRGrandChallengesforDisasterReduction.pdf, 2005.
13. Figge, S. and Rannenberg Kai.: Inviting new Players to the Multimedia M-Commerce Arena - An Approach to enhance the current M-Commerce business model with regard to emerging DVB-T networks, in L. E., P. B. and K. J. (Eds.), Mobile Information Systems, New York, USA, Springer, 2004, pp. 311-322.
14. Fritsch, L. and Scherner, T.: A Multilaterally Secure, Privacy-Friendly Location-based Service for Disaster Management and Civil Protection, Proceedings of the AICED/ICN 2005, Springer Lecture Notes on Computer Science LNCS 3421, Berlin, Heidelberg, New York, Springer, 2005, pp.1130-1137.
15. GSM association Location Based Services, Version 3.1.0, PRD SE.23, GSM Association, http://www.gsmworld.com/documents/lbs/se23.pdf , 2003.
16. Gomez, A. E., Passerini, K. and Hare, K.: Pubic Health Crisis Management - Community Level Roles and Communication Options, in B. Van der Walle and M. Turoff (Eds.), Proceedings of the 3rd International ISCRAM Conference, Newark, NJ, USA, 2006, pp. 435-443.
17. Grindley, P.: Standards Strategy and Policy, Oxford University Press, New York, 1995.
18. Gruntfest, E. and Huber, C.: Status report on flood warning systems in the United States, Volume 1, May 1989, New York, Springer, 1989, pp. 279-286.
19. Hagel, J. (I. I. I.) and Armstrong, A. G.: Net gain: expanding markets through virtual communities, Harvard Business School Press, Boston, MA, USA, 1997.
20. Hoffman, D. L., Novak, T. P. and Peralta, M.: Building consumer trust online, Communication of the ACM (42:4), 1999, pp. 80-85.
21. Katz, M. L. and Shapiro, C.: Network Externalities, Competition, and Compatibility, The American Economic (75:3), 1985, pp. 424-440.
22. Koelsch, T., Fritsch, L., Kohlweiss, M. and Kesdogan, D.: Privacy for Profitable Location Based Services, Proceedings of the Security in Pervasive Computing Workshop 2005, Boppard, Springer, 2005, pp. 164-179.
23. Kron, W. and Thumerer, T.: Water-related disasters: Loss trends and possible countermeasures from a (re-) insurers viewpoint, 3rd MITCH Workshop, Dresden, 2002.
24. Moores, T. T. and Dhillon, G.: Do Privacy Seals in E-Commerce Really Work? Communications of the ACM (46:12), 2003, pp. 265-271.
25. Munich Re Group: Risk Communication - What happens when something happens, Munich Re, Munich, 2002.
26. Munich Re Group: Knowledge series - Topics Geo Annual review: Natural catastrophes 2005, Munich, 2006.
27. National Geospatial-Intelligence Agency WGS84 - Its Definition and Relationships With Local Geodetic Systems, Third Edition, Amendment 1, Department of Defense World Geodetic System, 2000.

28. O'Connor, P. J. and Godar, S. H.: We know where you are: the ethics of LBS advertising: Mobile commerce: technology, theory, and applications, 2003, pp. 245-261.
29. PRIME consortium: PRIME - Privacy and Identity Management for Europe, https://www.prime-project.eu/, accessed 20-Feb-2007.
30. Rice, D. O., Garfinkel, R. S. and Gopal, R. D.: Security, Privacy, and the Trusted Information Intermediary, Proceedings of the Tenth Americas Conference on Information Systems (AMCIS'2004); New York, New York, August 2004, pp. 1403-1411.
31. Roßnagel, H. and Scherner, T. Secure Mobile Notifications of Civilians in Case of a Disaster, in H. Leitold and E. Markatos (Eds.), Proceedings of the 10th IFIP Open Conference on Communication and Multimedia Security (IFIP CMS 06), Berlin Heidelberg, Springer, 2006, pp. 33-42.
32. Scherner, T. and Fritsch, L.: Notifying Civilians in Time - Disaster Warning Systems Based on a Multilaterally Secure, Economic, and Mobile Infrastructure, in Proceedings of the Eleventh Americas Conference on Information Systems (AMCIS 2005), 2005.
33. Shapiro, C. and Varian, H. R.: Information rules: A strategic guide to the network economy, Harvard Business School Press, Boston, MA, USA, 1998.
34. Shneiderman, B. and Preece, J. PUBLIC HEALTH: 911.gov, Science Magazine (16:315), 2007.
35. Spiegel online: Datenschützer warnt vor Missbrauch, *Spiegel online,*, http://www.spiegel.de/netzwelt/mobil/0,1518,463814,00.html, accessed 02-March-2007.
36. Sxip Identity Corporation: Sxip identity, http://www.sxip.com/, accessed 02-Mar-2007.
37. Swiss Interbank Clearing; http://www.sic.ch/tkicch_home/tkicch_onswissinterbankclearing.htm, accessed 27-April-2007.
38. Turoff, M., Chumer,. M. J. and Hiltz, S. R.: Emergency Planning as a Continuous Game, in B. Van der Walle and Turoff Murray (Eds.), Proceedings of the 3rd International ISCRAM Conference, Newark, NJ, USA, 2006, pp. 477-486.
39. Vascellaro, J. E.: Social networking gets easier by cellphone, Wall Street Journal Europe 2007.
40. Voser, S. A.: http://www.geocities.com/mapref/dat/dat.html, accessed 25-Jan-2007.
41. Weitzel, T.: A Network ROI, Proceedings of the MISQ Academic Workshop on ICT standardization, ICIS, Seattle WA, USA, 2003.
42. Zibuschka, J., Fritsch, L., Radmacher, M., Scherner, T. and Rannenberg, K. Towards Privacy for Flexible Location-Based Services Enabling Dynamic Mobile Operator Business Models, in Proceedings of the 22nd IFIP TC-11, Sandton, South Africa, 2007.
43. blogger.com: Dutch test (CB) SMS disaster alarm, http://cell-broadcast.blogspot.com/2005/11/dutch-test-cbsms-disaster-alarm.html, accessed 26-Jan-2007.