# A Multilateral Secure Payment System for Wireless LAN Hotspots

Stephan Groß, Sabine Lein, and Sandra Steinbrecher

Technische Universitt Dresden,
Department of Computer Science,
Institute for System Architecture,
D-01062 Dresden, Germany
{st.gross, sl15, steinbrecher}@inf.tu-dresden.de

**Abstract.** Beginning with the adoption of the de-facto standard for wireless LAN communications IEEE 802.11 in 1999 we can observe a continuous growth of public wireless LAN hotspots that provide access to the Internet for modern road warriors. Unfortunately, current hotspots still suffer from several security drawbacks. In this paper we analyse how payment schemes used in current hotspot architectures consider the security requirements of both hotspot providers and subscribers. We identify a conflict between subscribers' wish for privacy and hotspot providers' interest in prohibiting unlicensed (and thus unpaid) usage of the hotspot as the most challenging security objectives a future payment system has to fulfill. As a solution solving this conflict we propose a multilateral secure payment system for wireless LAN hotspots based on electronic coins invented by David Chaum. As a side effect our approach also supersedes the sophisticated authentication techniques used in current hotspot implementations, thus, simplifying the roaming between different providers' hotspots.

## 1 Introduction

The last years have seen the vision of mobile computing becoming more and more true. Today, in many public places like airports, railway stations, restaurants or hotels so-called wireless LAN hotspots offer immediate access to the Internet using any IEEE 802.11 enabled device like a notebook or a PDA. Recent developments even go further and utilize wireless LAN technology to build Voice-over-IP enabled mobile phones as an alternative to common DECT or even GSM and UMTS based phones [1].

Wireless hotspot providers want their service to succeed now and in the future and to receive an economical benefit for their investments. This means providers necessarily have to assure that potential subscribers trust in their service and thus have to consider their requirements. Providers either are financed by external partners e.g., by advertising shown to the subscribers [2], or might charge a fee for the usage to the subscribers. In the latter case correct and non-repudiable charging of the used services is necessary. Thus, current hotspot systems put great effort in the accounting of generated traffic [3]. This is typically realized by utilizing common AAA (Authentication, Authorizing and Accounting) systems [4]. Unfortunately, this leads to a decrease of usability. Before one

S. Katsikas, J. López, G. Pernul (Eds.): TrustBus 2005, LNCS 3592, pp. 80–89, 2005.

can actually use a hotspot he has first to register with the hotspot provider. During registration the subscriber has to choose a payment method (e.g. credit card). Depending on the method chosen he has to provide detailed information about himself, e.g. his name and his credit card number. In return he receives some token from the hotspot provider (for instance a login name and a password) to legitimate himself at the hotspot. The services used by him are then taken into account by the provider and charged to him. Beside from the already mentioned usability aspects this procedure also suffers from a significant security drawback: combining the user data acquired during the registration phase with the data gathered at the hotspots facilitates the generation of detailed user profiles. Consequently, the lack of security is still seen as an obstacle of current hotspot systems by the majority of possible subscribers [5,6]. Wireless LAN Hotspots will only become successful if further efforts are taken to increase security, usability, interoperability and easy accounting of the service provided.

The integration of techniques and methods from other network standards like GSM, GPRS and UMTS [7,8,9] will help as well as the usage of Single-Sign-On authentication methods [10]. Multilateral security in GSM networks has been studied in detail (e.g., [11]), but so far no similar study exists for wireless LAN.

In this paper we propose a multilateral secure payment system for wireless LAN hotspots based on electronic coins that allows its anonymous but non-repudiable use. In addition it supports a better usability as it needs no complicated authentication mechanisms, therefore allowing easy roaming between different hotspot providers. In section 2 we start with a collection of the requirements the participants in a hotspot scenario have and come to the conclusion that the only potential conflict lies in the hotspot subscriber's wish of privacy and the hotspot provider's strong interest in accountability of usage, i.e. preventing unpaid use. Going on we classify the available payment methods and examine how far they fulfill the security requirements. In section 3 we describe the design of our multilateral secure payment scheme. Section 4 is dedicated to the prototype implementation in Java and section 5 to some concluding remarks.

## 2 Requirements Analysis

The parties involved in a wireless LAN payment system can be divided into two groups: the service providers and the subscribers. Speaking of the service provider we further distinguish [3] between:

**Hotspot Property Owner:** entity which provides the locality for a wireless LAN hotspot, e.g. the owner of a hotel or a restaurant.

**Hotspot Operator:** entity which provides a wireless network for public Internet access at hotspots, i.e. technical equipment, maintenance support and backbone connection.

**Clearinghouse:** entity which provides the measures needed to invoice the subscriber for the services he used.

In the following we ignore the hotspot property owner as far as he is not involved in the operation of the hotspot (e.g. by combination of both hotspot property owner and hotspot operator in one person) and not paid on a pro-rata basis depending on the profit realised. In the latter case he must be treated like a hotspot operator.

Accounting systems used in present hotspot architectures adopt the browser-based Universal Access Method (UAM) defined by the Wi-Fi Organization [3]. Thus, the subscriber can access a hotspot with only a Wi-Fi network interface and an Internet browser on his device. The functional part of such a hotspot consists of four phases:

**Registration:** Before a subscriber can access a hotspot he has to declare some static data (e.g., name, address, bank account) to a clearing house associated with the hotspot operator. The clearinghouse in return provides him with valid access data.

**Login:** To initiate a wireless Internet access at a hotspot one has to authenticate himself using the access data received during the registration. This leads to dynamic connection data collected by the hotspot operator for each session.

**Accounting:** So-called accounting events [12] trigger the hotspot to ascertain the accounting data from the connection data.

**Billing:** The hotspot operator transmits the accounting data to the clearing house which associates them with static data from the respecting subscribers, subsumes all accumulated accounting data and issues an invoice for the customer.

Figure 1 depicts the interaction of the involved parties with the accounting system and the corresponding data flows.

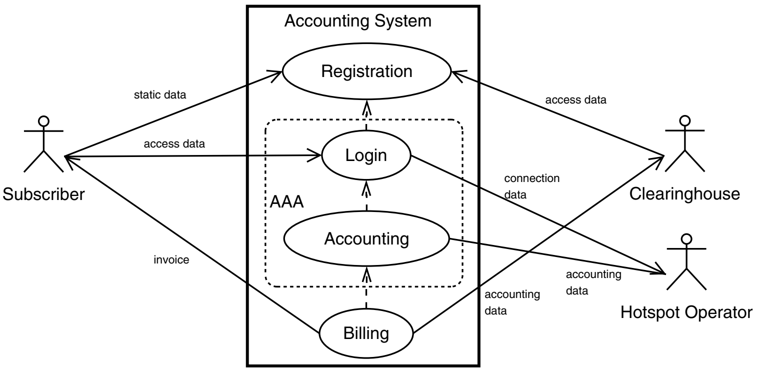


**Fig. 1.** Basic Functions of an Accounting System for Wireless LAN Hotspots

### 2.1 Security Requirements

Most of the involved parties' security interests are about the handling and separation of the data processed within the system. Due to the lack of space we only summarize their major issues briefly in table 1.

The most central conflict in the sense of multilateral security occurs between the subscriber's wish to minimize the amount of data transmitted and stored and all participants' interest to reach integrity and accountability of network usage that needs data to be stored as proofs. This conflict is already known from telephone accounts.

**Table 1.** Summary of all Participant's Security Interests

| | Subscriber | Service Provider | |
|---|---|---|---|
| | | Hotspot Operator | Clearinghouse |
| Authenticity of communicating partners | + + | + | + + |
| Confidentiality of transmission | | | |
| → Access data | + + | + + | + + |
| → Accounting data | + + | + + | + + |
| → Connection data | + + | ○ | ○ |
| Confidentiality of subscriber identity | + + | − − | − − |
| Confidentiality of location data | + + | − | − |
| Integrity of transmission | | | |
| → Access data | + | + | + |
| → Accounting data | + + | + + | + + |
| → Connection data | + | ○ | ○ |
| Accountability | + + | + | + + |
| Availability | + + | + + | + + |

+ + … great interest, + … normal interest, ○ … no special interest, − … dislike, − − … great dislike

### 2.2 Roaming

Beneath the security requirements roaming is one of the most essential features to make a business model for hotspots successful. Roaming means that the subscriber is a client of only one provider who makes agreements with other providers that the subscribers might use their infrastructure and the client's provider collects the money for this from his client. The usage of mobile phones has already shown that people travelling much have to use different providers to guarantee permanent reachability. When travelling through Europe by train permanent changes of providers occur but subscribers usually do not notice it in their reachability because of the roaming agreements between the different providers. In a similar easy way subscribers like to use wireless LAN hotspots. Independent of their current whereabouts and the provider of the access point at this place they like to use the respective existing network in an easy way. Requirements on and specification of possible roaming business models have been studied in [13].

### 2.3 Payment Methods

**Prepaid.** Prepaid payment needs no personal data to be gathered as static data, because the customer pays the provider in advance. Following multilateral security this fulfills both requirements of subscribers and providers: Unlinkability and anonymity of data can be realized easily as well as the risk of accountability can be transferred to the subscriber. The amount to pay will be booked to the subscriber's prepaid account with his begin of usage (and then in certain time or data units). If the credit balance the subscriber pays in advance is stored centrally at the provider the subscriber only holds the access data which he uses to identify himself within the login, e.g. by username-password-combination or a remote access card. If the credit balance is stored locally at the user's device or smart card it needs to be protected additionally against misuse by the user with physical measures. The payment needs signals from the provider to the user side. To control the other party the one not holding the credit balance must also log the usage of the service. Altough prepaid payments might be recharged they should only be used once to prevent the building of at least pseudonymous user profiles.

A special kind of local storage are anonymous digital coins [14] which try to implement the typical features hard cash has. They are issued by a bank and can be used independently from concrete merchants. The coins allow unlinkability of payments as well as anonymity of the subscriber using them as long as he only uses a coin once. This is realized by the usage of blind signatures. Unfortunately, there exists no practical system that implements all the above features, not to speak of efficiency of communication if taking this classical approach of anonymous digital coins.

For hotspot usage it is imaginable to save the communication with a bank if the service provider takes the role of the bank and issues coins that are usable at his hotspots and all other hotspots that allow roaming. The usage of coins in the login process supersedes other identification methods. While digital coins did not succeed in payment for non-digital items or services for the payment of digital services they can be a good solution because no change of medium occurs.

**Postpaid.** Postpaid payment necessarily needs the collection of connection data and the creation of accounting data as well as the storage of corresponding static data. Connection data can be deleted some time after the invoice and should be stored separately from the static data. Postpaid payment can also be combined with pseudonymous usage of the service if identity management systems guarantee the necessary accountability of subscribers to the service providers. But this solution would require an appropriate infrastructure to exist.

**Individual Accounting.** A fair solution for accounting is that every subscriber only has to pay the amount of data or time he used an access point. Technically the individual accounting will be realized by small time slices or data amounts that will be charged for fixed prices. This kind of accounting is applicable to both post- and prepaid payment. Especially the concept of anonymous coins exactly meets the necessary requirements.

**Flat Rate.** A popular model for internet usage are flat rates where subscribers get a certain amount of time or traffic he can consume for a fixed price. This business model is both applicable to pre- and postpaid payment. But only the unlimited amount of traffic makes the creation of connection and accounting data obsolete.

## 3 Design of a Multilateral Secure Payment System

Based on the security requirements and possible payment methods we present our design for a multilateral secure payment system. It is divided into a class model and several basic interaction protocols describing the static system architecture and the dynamic system behaviour respectively. We conclude this section with some remarks on the limitations of our approach.

### 3.1 System Architecture

The central requirements for a multilateral secure payment system identified in the previous section were the confidentiality and integrity of the transmitted access data as well as the concurrent confidentitality of the subscriber's identity and the accountability of the used/provided services. These requirements will be considered in the system architecture. Of course, availability aspects are of great importance as well, but due to the lack of space we have to postpone a detailed consideration for future work.

As we have stated in section 2.3 postpaid payments make the anonymous use of a hotspot more difficult. Thus, we base our system on prepaid vouchers that are used to transfer real money into electronic coins. In our prototype this transaction is performed by the subscriber and the clearinghouse. However, it can be easily extended with a third party acting as a bank to introduce universal usable coins instead of distinct currencies for each clearinghouse. Apart from the anonymity aspects our solution offers a second major advantage over current implementations: there is no longer a need for a complicated authentication phase at the hotspot. Hence, the roaming between different hotspot operators becomes more easy as you only have to check the validity of the coins spent.

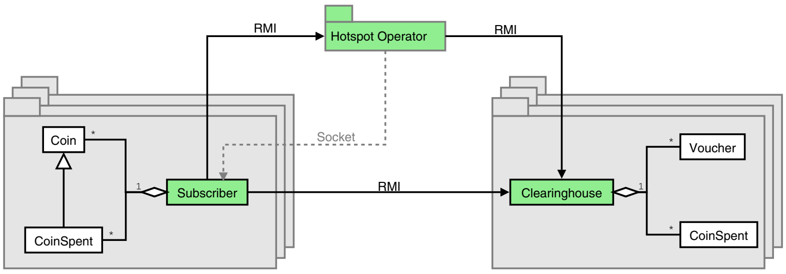


**Fig. 2.** Basic Architecture of our Payment System

Figure 2 gives an overview of our system architecture. It is basically divided into three subsystems, one for the subscriber, one for the hotspot operator, and one for the clearinghouse respectively. The directed connections indicate the interaction between the three parties. E.g. the subscriber has to cooperate with the hotspot to initiate a new session who again falls back on services provided by the clearinghouse to perform this task. The subscriber's main task is to manage the subscriber's purse whereas the clearinghouse cares about issuing and cashing coins. The hotspot operator's only task is to provide an Internet connection for the time paid by the subscriber.

### 3.2 System Interaction

Our system's interaction is defined by two central protocols: The *Withdrawal Protocol* to generate new coins, and the *Payment and Deposit Protocol* to initiate a new hotspot session. The entities in both protocols (*Subscriber*, *Clearinghouse*, *Hotspot Operator*) correspond to the partners described in Chaum's scheme [14]. Whereas the Withdrawal Protocol is more or less a direct adaption of the general model our Payment and Deposit Protocol is summarized in figure 3.

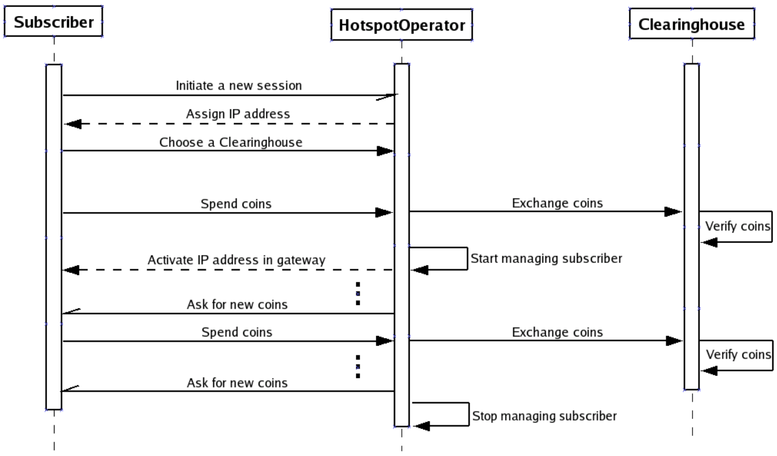


**Fig. 3.** The Payment and Deposit Protocol

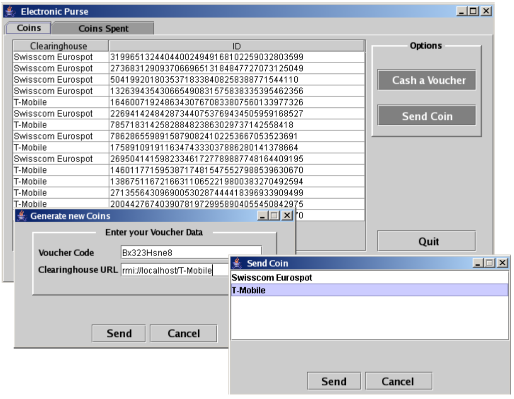
### 3.3 Limitations

There are some aspects we have left out in our current design for the sake of simplicity. First of all, as with every cryptographic system you have to care about the quality of the cryptographic tokens used. Thus, the codes used in our voucher based approach must be of sufficient length. Furthermore, we do not offer a solution against common hijacking and denial of service attacks utilizing forged deauthentication requests and IP address spoofing. The transfer of electronic coins between different devices of a subscriber as well as their protection against loss by theft or system failure is left for future work, too. The most important limitation of our design is probably its lack of formality. We deliberately tackled the problem stated in a more pragmatic way to show how easy one can build a system that respects the interests of all parties involved. Nevertheless, this approach does not consider some important aspects like the atomicity of the multi-party protocols used. For example, the coin generation and the payment protocol must be fair, i.e. no party taking part at these protocols should be cheated if the transaction fails because of system failure or fraud. Having said this, we still believe that our approach presents an important step-forward compared to the hotspot systems currently in use.

## 4 Prototype Implementation

Our prototype implementation is based on Java. The functionality is capsuled in four fundamental blocks as specified in the following subsections. For the concrete implementation of anonymous digital money we currently revert to the Lucre project [15], a Java-based implementation of a Diffie-Hellman variant on Chaumian blinding. Due to the modular structure of our implementation this can be easily replaced by another implementation. The purse is currently stored in an XML file on the subscriber's device. The subscriber's access to the Internet is regulated at the hotspot by reconfigurating the firewall settings of the underlying Linux system.

In addition to the functional part we have also implemented a simple graphical user interface for better usability. Figure 4 gives an impression of the subscriber's part of this interface. The main window represents the subscriber's purse. It is divided into two tabs, one for the coins already spent and one for those not. At a hotspot the subscriber chooses between the available clearinghouses and then spends the required amount of coins (see small window on the bottom right). The small window on the bottom left shows the process of cashing a voucher for new coins. Comparable interfaces exist for the clearinghouse and the hotspot operator.



| Clearinghouse | ID |
|---|---|
| Swisscom Eurospot | 319965132440440024949168102259032803599 |
| Swisscom Eurospot | 273683129093706696513184847727073125049 |
| Swisscom Eurospot | 50419920180353718338408258388771544110 |
| Swisscom Eurospot | 132639435430665490831575838335395462356 |
| T-Mobile | 164600719248634307670833807560133977326 |
| Swisscom Eurospot | 226941424842873440753769434505959168527 |
| T-Mobile | 7857183142582884823863029737142558418 |
| Swisscom Eurospot | 78628655989158790824102253667053523691 |
| T-Mobile | 17589109191163474333037886280141378664 |
| Swisscom Eurospot | 269504141598233461727789887748164409195 |
| T-Mobile | 146011771595387174815475527988539630670 |
| T-Mobile | 138675116721663110652219800383270492594 |
| T-Mobile | 271355643096900530287444418396933909499 |
| T-Mobile | 200442767403907819729958904055450842975 |

Enter your Voucher Data

Voucher Code: Bx323Hsne8

Clearinghouse URL: rmi://localhost/T-Mobile

Swisscom Eurospot

T-Mobile

**Fig. 4.** The Subscriber's GUI

## 4.1 Implementation of the Clearinghouse

The clearinghouse's interface declares several remotely accessible methods. The most interesting ones are *getNumberOfCoins*, *getAmount* and *processCoinRequest*. Whereas *getNumberofCoins* calculates the number of coins to be generated for a given valid voucher code and a fixed coin value, *processCoinRequest* is used to sign several raw coins as requested by a subscriber. Last but not least *getAmount* is called by the hotspot operator to transfer the signed coins given by the subscriber. The coin is checked for correctness and for resubmission. If both tests pass correctly the coin is marked as spent by storing its serial number and the available credit is returned to the hotspot operator.

## 4.2 Implementation of the Subscriber

The abstract class *Subscriber* represents the subscriber's device. Its main function is the administration of the electronic purse. The purse is filled by passing a valid voucher code and a corresponding clearinghouse address to the method *generateCoins*. The communication under the hood is realised with Java RMI. Later, the method *spendCoin* is used to initiate an Internet connection at the hotspot. First, it checks which clearinghouses are available (method *getClearinghouseList*). Then the so-called *SocketListener* is started. This class keeps the running connection under surveillance by opening a socket communication for signaling messages about the status of the connection, e.g. to inform the subscriber if he runs out of credit. Finally, the hotspot operator's method *dischargeCoin* is called to actually spend the coin and enable the Internet connection.

### 4.3 Implementation of the Hotspot Operator

The most interesting functions of the Hotspot Operator party are those initiated by the subscriber via RMI calls. This interface is defined in the class *HotspotOperator*. As already mentioned in section 4.2 the method *getClearinghouseList* delivers a list of all clearinghouse instances available at the hotspot. To establish an Internet connection the subscriber has to pay the necessary charge using the hotspot operator's method *dischargeCoin*. The hotspot operator processes this request (*processCoin*) by sending the handed over coins to the appropriate clearinghouse where the coin is checked for correctness and resubmission. If none of the tests fails the clearinghouse returns the corresponding credit to the hotspot operator who increases the subscriber's *SessionTimer* accordingly or opens a new subscriber session by reconfigurating the firewall settings on the hotspot's Internet gateway respectively. The class *SessionTimer* represents a thread initiated directly after a subscriber spends his first coin. It manages a socket connection to notify the subscriber about special system events such as ceasing credits.

### 4.4 Handling of Electronic Coins

For the sake of modularity the handling of electronic coins is capsuled in a separate package. This package provides all the functionality used by the subscriber and the clearinghouse during the generation of new coins. It basically contains three classes: *PublicCoinRequest* represents the blended and encrypted serial number of a coin to be signed. It is accompanied by its counterpart *SignedCoinRequest* that contains the matching signature. Last but not least, *CoinRequest* contains all encryption and decryption parameters known to a *Subscriber*, e.g. blending factor and serial number.

## 5 Conclusion and Final Remarks

We explained the wide agreement of all participants involved in a wireless LAN hotspot scenario concerning central security requirements. On the first view only the subscriber's wish for unobservability on the one hand and the provider's great interest in non-repudiable service usage on the other hand seem to conflict. With our prototype implementation we have demonstrated that this supposed conflict can easily be solved with the means of a multilateral secure system design. We strongly believe that our approach has the potential to put some new life into the domain of electronic cash as it does not suffer from drawbacks coming from exchanging virtual money with real goods. Instead, we use electronic coins to pay for the virtual good of using a wireless LAN hotspot. In addition, our system does not depend on AAA architectures like current systems do and thus, simplifies the roaming between different hotspot providers. For the future we plan to extend our prototype with more sophisticated features (e.g., distinct coin values and the support of electronic change) and evaluate it in a real world scenario.

## References

1. Stanossek, G.: Hotspots: Nische oder UMTS-Konkurrenz? VDI Nachrichten **41** (2003)
2. Jamaluddin, J., Doherty, M., Edwards, R., Coulton, P.: A Hybrid Operating Model for Wireless Hotspot Businesses. In: Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC 2004), Las Vegas, Nevada, USA (2004)
3. Anton, B., Bullock, B., Short, J.: Best Current Practices for Wireless Internet Service Provider (WISP) Roaming. Technical report, Wi-Fi Alliance (2003) Retrieved February, 14 2005 from `http://www.wi-fi.org/opensection/downloads/WISPr_V1.0.pdf`.
4. de Laat, C., Gross, G., Gommans, L., Vollbrecht, J., D.Spence: Generic AAA Architecture. RFC 2903, The Internet Engineering Taskforce (IETF) (2000) Retrieved February, 14 2005 from `http://www.ietf.org/rfc/rfc2903.txt`.
5. Buchwald, M., Greiber, K., Milosevic, F.: Hotspot Report – Der Praxistest. Industrial study, Detecon International GmbH (2003)
6. Balachandran, A., Voelker, G.M., Bahl, P.: Wireless Hotspots: Current Challenges and Future Directions. In: Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, ACM (2003)
7. Ouyang, Y.C., Chu, C.H.: A Secure Context Transfer Scheme for Integration of UMTS and 802.11 WLANs. In: IEEE International Conference on Networking, Sensing and Control (ICNSC 2004), Taipei, Taiwan (2004)
8. Chakravorty, R., Vidales, P., Subramanian, K., Pratt, I., Crowcroft, J.: Performance Issues with Vertical Handovers: Experiences from GPRS Cellular and WLAN hot-spots Integration. In: Proceedings of the IEEE Pervasive Communications and Computing Conference (IEEE PerCom 2004). (2004)
9. Haverinen, H., Mikkonen, J., Takamki, T.: Cellular Access Control and Charging for Mobile Operator Wireless Local Area Networks. IEEE Wireless Communications (2002) 52–60
10. Matsunaga, Y., Merino, A.S., Suzuki, T., Katz, R.H.: Secure authentication system for public WLAN roaming. In: Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots, ACM Press (2003) 113–121
11. Federrath, H., Jerichow, A., Pfitzmann, A.: MIXes in Mobile Communication Systems: Location Management with Privacy. In: Information Hiding. Volume 1174 of LNCS., Springer-Verlag Heidelberg (1996) 121–135
12. Beadles, M., Mitton, D.: Criteria for Evaluating Network Access Server Protocols. RFC 3169 (2001) Retrieved Feburary, 14 2005 from `http://www.ietf.org/rfc/rfc3169.txt`.
13. Verhoosel, J., Stap, R., Salden, A.: A Generic Business Model for WLAN Hotspots – A Roaming Business Case in the Netherlands. In: Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, ACM (2003)
14. Chaum, D.: Blind Signatures for Untraceable Payments. In: Advances in Cryptology - Proceedings of Crypto ’82, New York, Plenum Press (1983) 199–203
15. Laurie, B.: Lucre: Anonymous Electronic Tokens v1.8. Technical report (2003) Retrieved Feburary, 16 2005 from `http://anoncvs.aldigital.co.uk/lucre`.