J Comput Virol (2007) 3:185–194
DOI 10.1007/s11416-007-0049-x

EICAR 2007 BEST ACADEMIC PAPERS

# Transaction pseudonyms in mobile environments

**Oliver Jorns · Oliver Jung · Gerald Quirchmayr**

Received: 12 January 2007 / Revised: 7 February 2007 / Accepted: 25 March 2007 / Published online: 17 May 2007


**Abstract** Network Operators start to offer formerly hidden services such as location service, messaging services and presence services. This fosters the development of a new class of innovative context aware applications that are operated by third party application providers. However, without the implementation of proper privacy protection mechanisms, location and presence information, that is processed by third party application providers, may also imply severe risks to users. If no privacy protection is foreseen, the user's identity could be used maliciously which renders such applications dangerous. To protect the user's sensitive data such as location information we propose a novel service architecture which fosters the development of innovative applications that brings together internet applications with telco services. An underlying privacy enhancing mechanism that is based on the notion of pseudonyms allows even untrusted third party application providers to access sensitive data provided by telco services such as location, presence or messaging services. Due to their high security, pseudonyms guarantee that the user's identity is kept secret towards the untrusted application providers. Due to its low computational complexity this pseudonym generation scheme can also be implemented on devices such as mobile phones and digital assistants with only little computational power and restricted memory capabilities. To illustrate our approach, we demonstrate a transportation ticket application that implements the proposed service architecture. This application allows the use of transportation tickets which are extended by the location-tracking functionality. Similar to the well known paper based transportation tickets our solution supports anonymity of users even if the ticket application "knows" the location of the holder.

Oliver Jorns is a researcher at the Telecommunications Research Center in Vienna and is also a Lecturer at the University of Vienna. Oliver Jung is employed as a Senior Researcher at the Telecommunications Research Center Vienna. He is also member of ISO/IEC JTC1 SC27 (IT security techniques). Gerald Quirchmayr is Professor at the Institute for Computer Science and Business Informatics at the University of Vienna and since January 2005 he heads the Department of Distributed and Multimedia Systems, Faculty of Computer Science, at the University of Vienna.

O. Jorns (✉) · O. Jung · G. Quirchmayr
Telecommunications Research Center Vienna (ftw.)
Donau-City Strasse 1, 1220 Vienna, Austria
e-mail: jorns@ftw.at

O. Jung
e-mail: jung@ftw.at

G. Quirchmayr
School of Computer and Information Science,
University of South Australia, SA-5001 Adelaide, Australia
e-mail: Gerald.Quirchmayr@unisa.edu.au

G. Quirchmayr
Institute of Distributed and Multimedia Systems,
University of Vienna, Liebiggasse 4/3-4, 1010 Vienna, Austria
e-mail: Gerald.Quirchmayr@univie.ac.ac.at

## 1 Introduction

Today, the realisation of ubiquitous computing as it was envisioned by Weiser [20] is far from reality. However, the fast technological development of mobile phones' and digital assistants' capabilities in terms of processing power and communication such as WLAN and Bluetooth also reflects the evolution of a new class of context-aware applications and services. For the first time it is possible to take into account the user's position as well as the position of other moving user's devices as well as static objects.

One essential factor for the success of such new services lies in the network operators' domain. The recent development of mobile services is even fostered by network operators

that start to open their networks to provide formerly hidden services to third party application providers. The effect is that due to standardized interfaces such as Parlay X 2.0 [15] application providers are no longer segregated from the network operators' formerly hidden location, presence and messaging services.

Today there are many different kinds of location-based services available on the market. The most popular systems use GPS data to display the actual position, calculate routes and provide additional information for travellers and tourists. Another class of location-based services receives location information directly from the network operator. Since each network operator stores all information of each user in a central database called home location register (HLR), neither additional devices such as GPS receiver, nor dedicated software running on the mobile device need to be installed. Meanwhile there are many different applications available which use the location information of mobile devices received directly from the network operator.

Another big driver of location-based services in the US market is the E911 mandate which prescribes that in emergency cases also location data has to be provided. Generally, one reason why the E911 finds more approval than other location-based services is because the actual location information is associated with the identity information of the respective person. In case of E911 it is even desired to bind the identity information to the location information of the person. Otherwise it may be impossible to provide help in adequate time.

For example, in case of an accident when it is a matter of life and death it is essential to receive as much information as possible such as the blood type or whether the person has diabetes or not in the shortest possible time. Of course, applications that may provide sensitive information also reach deeply into the private sphere. That is why adequate privacy protection mechanisms are essential.

Applications that are available to civil population may raise even more severe problems since misuse may end up even in potential danger for the relevant person. There are applications available that for example allow curious people watch their spouse or track friends. Such applications often require once-only consent of the user that is going to be watched. And even if the operating company canvass customer with the assertions that each localisation is based on mutual confidence between brides and pair of lovers, on second thoughts it shows that the business model is solely based on the uncertainty and curiosity of its customers. What was initially meant as a demonstration of faithfulness turns into suspiciousness and finally detachment.

Also from the system design point of view there are some defiances that have to be mastered in order to be able to provide user's security and privacy. During the registration process the person that shall be located has to give her consent. In case only once-consent is required the service can be easily misused by family members or colleagues or in general by anyone who can take the mobile device of somebody else in safe keeping at least for the duration necessary to send the localisation confirmation message. It is therefore crucial that the system is designed in such a way that all persons for whom at least one localisation process is activated receive from time to time a reminder message. This ensures that nobody can be located without given consent or knowledge.

Another requirement is that users shall be informed about each single location request. However, if users receive a notification message or a request for confirmation every time their location is requested this would become annoying very quickly. So, on one hand the system must provide means that allow users to grant permission to all subsequent location requests. On the other hand it must provide simple and free of charge measures that even prevent temporarily from processing of location data.

Of course, the abovementioned requirements pertain to only a very small subset of all codified requirements. The legal aspects shed light on the requirements of nowaday's and future's novel location-based systems and what has to be considered for implementation.

To protect users' concerns Price [16] states that it is important to design systems jurisdiction aware. This is not easy to achieve since privacy regulations may change and it is difficult to design a system that easily copes with all required changes.

The European Union Data Protection Guideline Directive 95/46/EC [5] represents a good guideline and discusses in particular the confidentiality and security (Article 16) as well as the processing of data (Article 17). The Directive 2002/58/EC [6] is an extension and describes traffic data explicitly as "*any data processed for the purpose of the conveyance of a communication channel on an electronic communications network or for the billing thereof*". Location data is described as "*any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user or a publicly available electronic communication service*". As already mentioned above, the important requirement that users have to be informed whenever a location request occurs and that they are regularly reminded about who is allowed to request location information and what is most important that the system is designed in a way that these notifications do not annoy users can clearly be concluded from these directives. To be more precise, the EU Directive [6] requests that data is under the sole control of the owner. This includes that the owner must be informed about the time span of location data usage as well as if data is processed by any third party providers.

The situation becomes even more complex if data has to be exchanged also with other countries, possibly even outside the EU. The EU Directive [6] therefore defines the so

called "transitive closure". As Price [16] states, this directive prescribes that it is only possible to exchange data with countries that have the same data protection guidelines or under the assumption of special contract. However, at the moment no EU Directive provides sufficient privacy protection on a global scale but as Fischer–Hübner [8] further states many countries outside the EU such as e.g. Canada adapted their new laws to be compliant to with the EU Directives.

In the following we give an overview about related work in the field of digital pseudonyms used for privacy protection. We continue with a description of the system architecture and each of the components which is followed by an explanation on the proposed pseudonym generation scheme which includes a detailed description of how transaction pseudonyms are generated. We further discuss security and performance issues and show how the system reacts on different disturbances. An example of a transportation ticket application shows the applicability of the transaction pseudonym scheme. Finally, we wrap up with conclusions.

## 2 Related work

Research on privacy for location-based services can basically be divided into techniques that are primarily based on privacy-policies and those, which are used to make location information anonymous, or rather blur location information. Treu [19] further states, that solutions that are based on privacy-policies presume that users have to trust their carrier to a certain degree. In the same regard another disadvantage is that it is difficult for users to control the adherence to privacy rules and policies. Their proposed solution uses anonymisation in the sense that instead of global positions only relative distances between users are used. By dint of shared keys members of communities shall be able to change their location information through distance-retentive transformations of coordinates.

Hash values as pseudonyms were first used by Lamport [13]. The security strength lies in the pre-image resistance of hash functions like e.g. MD5 or SHA-1/2 which further means that it is impossible to find the value of $x$ of a secure hash function $y = h(x)$ if only y is given. For $n$ authentications this authentication scheme first computes a chain of hash values $h^0, \ldots, h^n$. The last value ($n$th hash value) is then used for the first authentication. Each successive authentication uses the respective next hash value that is the $h^{n-1}, h^{n-2}, \ldots$ and so on till $h^0$ is reached. The pre-image condition of hash values provides that it is not possible to calculate in advance the respective next pseudonym. Despite its elegance this authentication scheme has the disadvantage that it requires $n * (n + 1)/2$ hash value calculations. This means the more authentications, the computational overhead increases. As we see later the computational overhead renders this scheme rather unusable on mobile devices with only little computing power and memory capabilities.

Rodden et al. [17] propose another solution that is also based on pseudonyms. Here, users are in charge of randomly generated pseudonyms which give them control over which third party application providers have access to their location information. Therefore, users store their location information together with a time stamp and an associated pseudonym at a location server. Third party providers that do not know the actual pseudonym are not able to access location information. Each user is in charge of who may access location information by simply changing the respective pseudonyms.

Kölsch et al. [12] introduce four different scenarios for privacy protection in location-based services. One of these scenarios is called intermediary scenario and describes a location intermediary that collects localisation information received from different sources such as the mobile operator or from the user who provides GPS coordinates. In this scenario the application's location intermediary acts as location broker which offers distinctive advantages such as access to different location sources in a unified and by the same token correlation of multi-source location information which results in better quality of the location data. Through the use of distinct pseudonyms. The disadvantage of this system is the use of asymmetric cryptography which results in higher computational costs and therefore is a barrier to some mobile devices.

Another solution proposed by Gruteser et al. [9] and Cheng et al. [3] uses location cloaking which is based on the concept of $k$-anonymity. This means that in a certain time interval at least $k$ users are within a certain rectangular area. A user is $k$-anonymous if his location cannot be distinguished from the location of the $k - 1$ other users.

Schulzrinne [18] defines a message format that allows transport of authorisation policy rules. This is used to support different location data transformations so that it is possible to adjust the resolution of location information and make authorisation decisions that are based on the current location.

## 3 System architecture

In this section we discuss the system architecture as it is depicted in Fig. 1. It consists of three major components, the client application, the third party application provider and the network provider. Each of these components implements a number of software modules. The glue that ties these components and its modules together is our mechanism based on pseudonyms. This combination allows the development of context-aware, location-based services without the loss of user's privacy. We discuss this pseudonym mechanism in detail in one of the following sections. In the following we start with a detailed explanation of each of the system's blocks and its components.

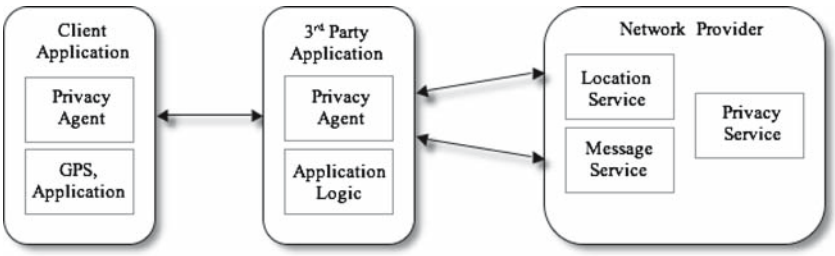


**Fig. 1** System architecture

### 3.1 The client application

The client application can be either a J2ME implementation for Java enabled phones or any other software implementation that runs on mobile phones such as Symbian or PocketPCs. The major software modules of this component are the applications' logic, a GPS receiver module and the so-called privacy agent module. Its responsibility is the generation and administration of digital pseudonyms. The primary function of each pseudonym is to authenticate the requestor. As we explain later in more detail, each pseudonym further expresses a unique relationship between the requestor and another identity. The privacy agent module is further implemented by all third party applications. Each privacy agent represents the client side implementation of the network providers' privacy service. Basically, the main task of the privacy agents and the network operator's privacy service is the exchange and verification of pseudonyms according to a predefined mechanism which we explain in detail in a later section.

The client application implements also a module that allows users to control the applications' behaviour. It implements the graphical representation of the application and allows users to interact with the system. The application module further communicates with other modules such as the privacy agent and the GPS module and controls conveyance of location data to the location service.

### 3.2 The third party application provider

The application provides a privacy agent and uses pseudonyms to authenticate itself. Unlike users' privacy agent it generates so called self-identifying pseudonyms. This special kind of pseudonyms is technically equal to the pseudonyms used by the users' privacy agents but with the difference that they are used by the network operator's privacy service for authentication purposes only. Each application provider therefore shares at least one contractual relationship and a shared secret with the network operator. Application provider may implement various applications such as the one described by Jorns et al. [10] which realizes a transport ticket system with location support. We discuss this example application briefly in a later section. In general, application providers may also requests resources from other applications such as map or route services but there are also many other applications conceivable such as location-tracking assistants that incorporate also other context data than location such as presence information.

### 3.3 The network provider

Network providers maintain huge infrastructures in order to provide their customers the ability to make phone calls, exchange of text messages and data transmissions with mobile phones and PCs. This complex infrastructure comprises amongst others location, messaging or presence services which access sensitive user data such as the user's location. The location information of every mobile user device is stored in the home location register (HLR) that is a central database operated by each network operator. It stands to reason that network operators treat sensitive information like location information very carefully and explains why current existing location based services provided by mobile operators are mostly not connected with third party applications.

However, with techniques that guarantee the protection of data and users' privacy such as the digital pseudonyms network operators may change their attitude and hopefully start to offer access to formerly hidden services via already existing standardized interfaces. The Parlay 2.0 [15] specification provides a number of interfaces to different kinds of network services.

### 3.4 Location service

The network operators' location service represents an interface between the customers' mobile devices, the application providers and the respective network operators' central database called home location register (HLR) which stores location information of all customers that are connected to the mobile network. The precision of the location information provided by the home location register varies and depends on the respective area. Whereas localisations of persons in rural and suburban areas provide only very low precision location information, localisations undertaken in urban areas can absolutely be used for applications such as those

mentioned by Treu [19] that consider only single persons who are registered to certain areas.

However, precise location information with accuracy up to only several meters can be reached with GPS. Hence, applications that rely on high precision location information require that the location service is flexible enough not only to provide cell-based localisations but also cope with location data that are sent from users directly. Meanwhile a growing number of users are equipped with mobile phones with integrated GPS receivers. Hence, it is conceivable to enable location services for technologies such as RFID, WLAN or Bluetooth but these are not discussed here.

As a result, the location service has to react dynamically according to different locations and actions of the users. For example, consider a user's mobile with enabled GPS module allows to send location information in constant intervals to the location service. As the user approaches the next underground station, satellite link is broken. Thereupon, after a certain time interval the location service switches to cell-based localisation. Even though the accuracy of the location data is now much more imprecise than it was when GPS data was provided, it is still good enough to track the user since every underground station is equipped with network antennas. As the underground antennas are located in underground stations applications can precisely distinguish between two almost identical locations since some are known to be underground. In case of transport ticket applications such as the one described in this work such distinctions may be helpful.

### 3.5 Message service

Depending on the respective application at hand users shall be informed about when they enter or leave a certain pre-defined area or if buddies with the same interests are in the vicinity. In either case users shall be informed asynchronously about the current state. The most efficient way is to use the short message service (SMS) in combination with the MIDP 2.0 Push Registry (2002) that is implemented by the mobile device. The combination of SMS messages and the MIDP 2.0 Push Registry has the advantage that the user does not need to start any application in order to receive messages. A received SMS messages can even start applications and induce further actions. The most important advantage why messages should be sent via legacy message systems is its simplicity. The operator can contact every user as long as he knows the Mobile Subscriber-Integrated Service Digital Network Number (MSISDN), which is always the case.

### 3.6 Subscription service

This service is accessible through a web-based interface and allows users to administer their personal data that includes the buddy lists. Furthermore, this service allows users to manipulate their privacy policies. In the strict sense, users have access to the privacy service to define who may request their location and when as well as how or if they may be notified about certain states. The subscription service is also called in case of errors such as out-of-sync pseudonyms and initiates re-initialisation of pseudonyms when necessary.

### 3.7 Privacy service

The privacy service is the server side implementation of the users' and applications' privacy agents. It administers all pseudonyms of each user and application and keeps track of any pseudonym change. The privacy service merges all information about all users. It stores who is the watcher of whom and which pseudonym is necessary to enable the location service to deliver location information. Furthermore, it maintains privacy policies of each user that may be edited through the subscription service. It is the only service that can map a valid pseudonym to a MSISDN. Thus, it can be seen as the core of the system where all information about users merges. It accesses other core databases of the system as needed to receive e.g. the MSISDN.

## 4 Generation of transaction pseudonyms

Our proposed pseudonym generation scheme uses the keyed hash function HMAC as underlying cryptographic mechanism. This function denoted as $h_k$ is depicted in (1). It shows how to build a chain of hash values by consecutively applying the hash function $h_k$ on the input $r$ that is initially a random number.

$$h_k^i(r) = h_k(h_k^{i-1}(r)), \qquad i = 1, 2 \ldots \tag{1}$$

The security of the system mainly relies on the security of the pseudonym generation scheme that we discuss in detail in the security section. The following section shows how pseudonyms are initialised.

### 4.1 Pseudonym initialisation

In principle we distinguish two different kinds of pseudonyms. One kind we call self-identifying pseudonyms. This allows users to securely request information that is bound to their own actual position. The second kind of pseudonyms we denote as presentity transaction pseudonym or, in case it is generated by third party application providers the so-called application transaction pseudonym. We use the term presentity from the presence terminology. The presentity denotes the person that can be located by another person—the person who requests the location is called the watcher. In case of self-identifying pseudonyms the user is the watcher and the

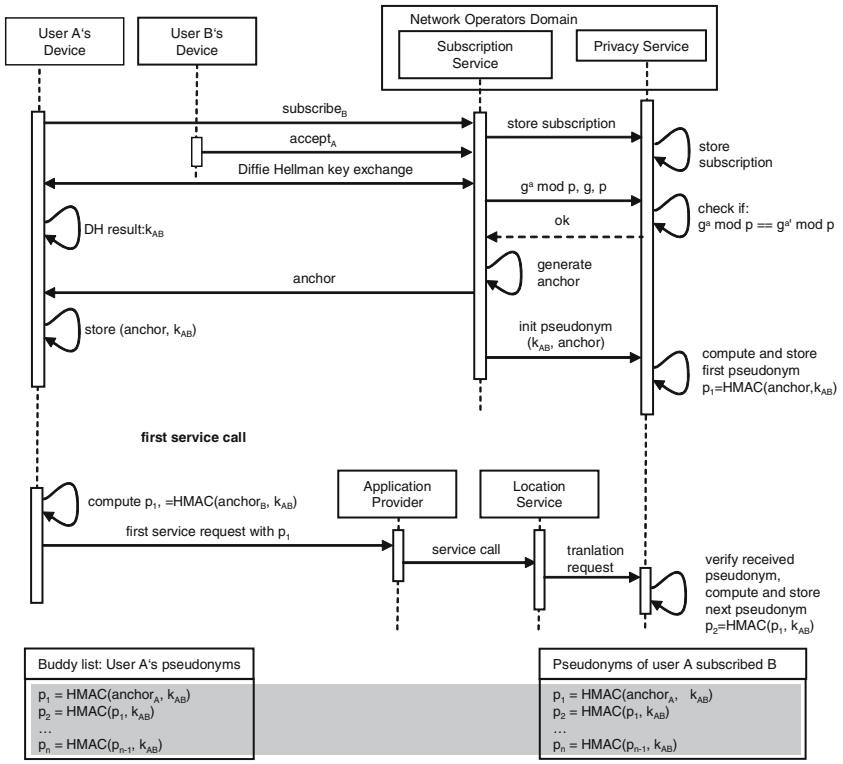


**Fig. 2** User subscription, pseudonym initialisation and first service call

presentity likewise. Both pseudonyms, the self-identifying as well as the presentity transaction pseudonym can only be translated by the privacy service to the respective user's identifier, which is the MSISDN. Except for differences during the subscription phase, the initialisation procedure of pseudonyms is equal (see Fig. 2). We discuss the difference in detail in the following paragraph.

**User subscription**. Before the subscription, the user's client allows to browse and search for other users listed in dedicated directories. Each user may choose one or more alias names. This is almost equal to existing subscription procedures of well known messaging systems such as e.g. Jabber.

As depicted in Fig. 2, user A first selects user B's alias and then sends a subscription request ($subscribe_B$) to the subscription service. The request is forwarded to the privacy service where all user subscription states and relationships are stored. When user B polls for pending subscriptions it receives the message that user A attempts to subscribe. If user B accepts, the subscription service initiates an update of the subscription state at the privacy service. The next time user A polls for the subscription state, the subscription service initiates a Diffie Hellman [4] key exchange with user A on behalf of the privacy service. The resulting secret key is used for the calculation of those pseudonyms that are related to user B. According to the Diffie Hellman protocol the subscription service eventually receives $g^a$ mod $p$ from user A. Whereas $g$ and $p$ are public parameters which can be exchanged in clear the parameter $a$ is user A's master password which was chosen by the user during registration at the network operator. The password is also stored securely by the network operators' privacy service and is not changed at any time except the user does this on purpose. However, the Diffie Hellman key exchange does not provide user authentication. This is why once the subscription service receives $g^a$ mod $p$ it cannot verify if this was really sent by user A. In order to prevent from man-in-the-middle attacks the subscription service forwards $g^a$ mod $p$ together with the public values $g$ and $p$ of the protocol to the network operators' privacy service that is in charge of user A's master password. Hence, it may prove the authenticity of the user who sent $g^a$ mod $p$ by recalculating $g^{a'}$ mod $p$ where $a'$ is the master password of user A stored by the privacy service. If $g^a$ mod $p$ is equal to $g^{a'}$ mod $p$ the subscription service receives from the privacy service that the users authenticity could be verified. By the way, it was neither necessary to exchange the user's master password nor any other identifier for the verification. Even though the Diffie Hellman key exchange protocol may be time and bandwidth consuming, it solves two problems at the same time. First, the generated secret key can be used for the consecutive generation of pseudonyms—we denote this key from now on as a derived secret key—and as described above with the user's master password it is even possible to verify the authenticity without any modifications or extensions. Furthermore, the Diffie Hellman key exchange protocol has to be processed only once for each user subscription which relativises the overhead. For the sake of simplicity and readability from

now on we denote the derived secret key as $k_{AB}$ instead of $(g^a \bmod p)^b \bmod p$ or $g^{ab} \bmod p$.

Now, user A receives from the subscription service a random string which we call anchor. A random number generator generates the anchor. The anchor and the derived secret key $k_{AB}$ are both stored on the user's device. The privacy service uses the anchor and $k_{AB}$ to generate and store the first transaction presentity pseudonym $p_1 = \text{HMAC}(\text{anchor}, k_{AB})$. As already mentioned, the calculation of self-identifying transaction pseudonyms is technically similar. The only difference is that in this case the users do not need to query for other users before they initiate the subscription process. Instead, the generation of self-identifying transaction pseudonyms can be initiated during the bootstrapping.

**User initiated service calls**. After the subscription has completed, users may request services from applications. In this example we assume that user A simply asks for the location of user B. As user A selects the appropriate buddy name from the buddy list, the software accesses the stored anchor and the appropriate shared secret $k_{AB}$ for this user and generates the first pseudonym $p_1 = \text{HMAC}(\text{anchor}, k_{AB})$. This pseudonym can be used now to request the location of user B. The third party application provider forwards the pseudonym to the location service of the network operator.

Upon receipt the privacy service eventually translates the pseudonym into the respective MSISDN whereupon the location service may initiate a cell-based localisation. For each subsequent service call, the network operator's privacy service calculates in advance the respective next pseudonym and stores it in the database. Both, the client's privacy agent as well as the network operator's privacy service must process pseudonyms in a synchronous manner. It is important for the correct functioning of requests that these pseudonyms are always synchronous. If pseudonyms run out of sync, the corresponding request cannot be processed. The problem of out-of-sync pseudonyms is discussed in detail in the security section.

## 5 System security and performance considerations

Pseudonyms are a useable way for the protection of the user's identity. However, if pseudonyms are deployed in a wrong way the user's identity cannot be protected sufficiently. In order to maintain a high security level a stringent requirement is that pseudonyms must change frequently. This implies that if the pseudonyms are static, an attacker might be able to determine the respective real world identity. Beresford [2] concludes that static pseudonyms do not provide sufficient privacy protection. We solve this problem by generating a new pseudonym for each request. The disadvantage is that we therefore have to accept additional computational costs. However, compared to other solutions that are based on public key cryptography or digests that are applied in reverse order like the authentication scheme of Lamport [13] the computational overhead is much lower.

### 5.1 Performance considerations

In this section we present some performance measurements that contrast the use of Lamport's authentication scheme to our proposed pseudonym generation scheme. Therefore we implemented the most widely deployed MD5 and SHA-1 as well as the HMACs with MD5 and SHA-1 as the underlying MACs.

The results of the HMAC measurements are shown in Table 1. Each value in this table represents the mean value of 100 calculations. For this test we used the J2ME Wireless Toolkit 2.0 emulator with an emulated VM speed of 100 byte code instructions per millisecond.

The first column shows how much time elapsed for the calculation of a single MD5 and SHA-1 as well as HMAC/MD5 and HMAC/SHA-1 hash value. The second and third column of the first two rows show the time that is necessary if the authentication scheme of Lamport were applied for 10 and 100 authentications. Since this authentication scheme requires $\frac{n\times(n+1)}{2}$ hash value calculations accordingly more computation circles are necessary. As the results show, compared to the HMAC implementations, the computational overhead increases significantly. The computational gap increases in such a way that Lamport's authentication scheme renders useless on mobile devices.

## 6 Security of message authentication codes

One important security aspect resides in the pseudonym generation scheme. We discuss the underlying cryptography used for the generation of the transaction pseudonyms that is the Keyed-Hash Message Authentication Code HMAC by Bellare et al. [1]. This hash function is constructed in the following way. It uses an input $r$, a secret key $k$ as input and a hash function such as MD4/5 or SHA-1/2 to generate the keyed-hash message authentication code.

Concerning the security of hash functions Menezes et al. [14] mention the following general requirements:

- Pre-image Resistance: given a secure hash function $h(x) = y$ it is impossible to find $x$ for the given hash value $y$.
- Second Pre-image Resistance: it is computationally impossible to find two different values $x_1, x_2$ such that $h(x_1) = h(x_2)$.
- Collision Resistance: it is computationally infeasible to find a pair $x_1$ and $x_2$ such that $h(x_1) = h(x_2)$.

**Table 1** User subscription, pseudonym initialisation and first service call

| Function | Computation time for single authentication | Computation time for ten authentications | Computation time for 100 authentications |
|---|---|---|---|
| MD5 | 51 ms | 2,190 ms (2.19 s) | 205,003 ms (∼3.4 min) |
| SHA-1 | 139 ms | 6,677 ms (6.667 s) | 701,950 ms (∼11.7 min) |
| HMAC/MD5 | 164.1 ms (0.164 s) | | |
| HMAC/SHA-1 | 448 ms (0.448 s) | | |

As stated by the authors of the position paper of ECRYPT [7] the security of HMAC relies on the security of the respective underlying hash function. Given a keyed hash function $y = h_k(r)$ an attacker would be able to calculate the output $y$ without knowledge of the secret key by either finding a collision of the underlying hash function or by finding the output of the compression function with a random and secret initial value.

With the use of SHA-2 these attacks are currently not accomplishable. Furthermore, at the time known collisions of other hash functions do not show any significant implications on the security of the HMAC scheme. Hence, it can be assumed that the HMAC is secure.

## 7 Out-of-sync pseudonyms

Another problem that may occur is that of pseudonyms that out-of-sync. That is when the network operator's privacy service receives a pseudonym that cannot be allocated to a certain identity of a person. This does not necessarily indicate a severe problem or an attackers attempt to compromise the system. There are at least two further reasons why this may happen.

- The pseudonym was changed due to a transmission error or for another unknown reason.
- The user induces a re-initialisation procedure.

In the first case, the privacy service receives a pseudonym that cannot be found in the database and wrapped to the respective user identifier. The privacy service therefore responds with an error message propagated back to the user's device whereupon the user's privacy agent initiates a new subscription request. However, the privacy service identifies this request as redundant since this subscription was already accepted before. Depending on the user's preferences thereupon a new shared secret may be exchanged between the user's privacy agent and the privacy service. Further, the privacy service generates a random number, which is also transferred to the privacy agent.

As soon as both, the privacy service and the privacy agent, agreed upon the new shared secret and the privacy service has sent the new random number to the privacy agent, the privacy service may calculate the first pseudonym in advance and store it in its database. For the next service request the client uses the random number it just has received as well as the newly generated shared secret for the generation of the next pseudonym.

It is possible, that the user herself decides to re-initialise the pseudonym chain. In this case, the privacy agent sends a dedicated request, which initiates the negotiation of a new pseudonym with the privacy service. After that, it also receives a new random number from the privacy service. From this moment on, the pseudonym mechanism is re-initialised and the client may request the next service call.

In the first case, the pseudonym is out-of-sync for an unknown reason whereas in the second case the user's privacy agent induced the re-initialisation. The re-initialisation frequency may depend on different factors. It makes sense to induce the re-initialisation procedure only for those pseudonym chains that are frequently used. This rather simple update scheme prevents from unnecessary traffic and further reduces computation efforts. It also relieves the user from the effort to change its password providing additional security to the users.

## 8 Position-aware and location-tracking applications

Our explanations so far concentrated exclusively on position-aware applications that provide information related to the current location of a requester. In this special case, the receiver of this information is the same person who sends the request. Junglas [11] discusses position-aware and location-tracking applications and distinguishes these by the role of the requestor. Location-tracking services allow location information to be collected and processed by, e.g. third party application providers on behalf of the requesting user. In this spirit, our system architecture also supports third party applications that collect, monitor and process location information that are periodically received from the location service. Depending on the respective third parties' application logic, this long-term process may theoretically run forever.

In long-term localisation processes where at least one or more buddies at the same time as well as the requester herself are involved, the third party application instead of the requesting user listens for location updates that are sent from the


**Fig. 3** Ticket application (client)

location service. After initiation of such a long-term process the user's privacy agent, the third party application and the network operator's privacy service share a so called session-identifier. The initiator of a long-term process receives this session-identifier as an acknowledgement that the long-term localisation process has been started successfully. The session-identifier can be used to terminate active processes ahead of time and to add or remove buddies from active localisations. It is further used by the location service for the administration of a localisation schedule that records which person shall be localised at what time. The privacy service as well as the third party application provider uses the session identifier to administer long-term localisations.

### 8.1 Transportation ticket example

One application that represents a viable example for location-tracking applications is the transportation ticket. The third party application does not only issue and administer transportation tickets but does also processes location information of the respective users. With the help of pseudonyms, the real identity of the ticket holder is unknown to the ticket application. Alike the well known worldwide deployed paper based transportation tickets this kind of ticket provides not only the user's privacy but allows the exchange of one or more tickets even if the selected receiver of the ticket is not in the vicinity of the sender.

What makes this ticket application really interesting is that once a ticket is activated the actual location of the ticket bearer can be used to send her additional information such as when to change or when the next train will arrive to name only a few. Figure 3a shows the menu that allows users to first choose their preferred kind of ticket. In this case the user selects a route ticket whereupon she is asked to enter the departure as well as the arrival station (see b, c). The received route details can also be browsed on the mobile. As depicted in Figure 3d and e particular stations of the route are displayed as bordered section. They may contain information about which transport to choose, the direction as well as the estimated time of departure. Furthermore, it is possible to load a map of the respective station area (see f).

## 9 Conclusions and future work

In this paper we have presented a solution that allows third party application providers to request and process location information of mobile users without the need to disclose the user's identity. The proposed architecture demonstrates the integration of internet technology with telco services that offer dedicated services such as location. The proposed architecture allows both, position-aware and location-tracking applications. The user's privacy is protected by secure pseudonyms that are based on HMAC and can also be implemented on mobile devices with only low processing power and memory capabilities. Compared to other authentication mechanisms we showed that our scheme does not even require much processing power.

The current status of our middleware allows us to test different scenarios of position aware and location-tracking applications. The implemented transportation ticket application is one example for a location-tracking application. We show that it is possible to integrate external services for route calculation as well as a payment service that allows users to access pre-paid accounts.

Next we want to extend our current transportation ticket system by additional information services. Users shall be informed in real time about traffic conditions on their route and possible alternative routes. Furthermore, the privacy service shall be extended by privacy policies to allow users to create and maintain also fine-grained access rules themselves.

## References

1. Bellare, M., Canetti, R., Krawczyk, H.: Keying hash functions for message authentication. In: Koblitz, N. (ed.) Advances in Cryptology—CRYPTO'96. Lecture Notes in Computer Science, vol. 1109, pp. 1–15. Springer, Heidelberg (1996)
2. Beresford, A.R.: Location privacy in ubiquitous computing. In: Technical Report 612. University of Cambridge, Cambridge (2005)
3. Cheng, R., Zhang, Y., Bertino, E., Prabhakar, S.: Preserving user location privacy in mobile data management infrastructures, in sixth workshop on privacy enhancing technologies (PET'06), Cambridge, UK (2006)

4. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Soc. 22(6), 664–654 (1976)
5. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 23 November 1995. Off. J. Eur. Commun. L 281, p. 31
6. Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 12 July 2002. Off. J. Eur. Commun. L 201/37
7. Network of Excellence in Cryptology IST-2002-507932. Recent Collision Attacks on Hash Functions: ECRYPT Position Paper. Revision 1.1, 17 February 2005, http://www.ecrypt.eu.org/documents/STVL-ERICS-2-HASH_STMT-1.1.pdf (last access: 2007-04-04)
8. Fischer-Hübner, S.: IT-security and privacy-design and use of privacy-enhancing security mechanisms. Lecutre Notes of Computer Science, LNCS, 1958. ISBN 3-540-42142-4. Springer, Heidelberg (2001)
9. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of The First ACM/USENIX International Conference on Mobile Systems, Applications and Services (MobySys), San Francisco, USA, pp. 31–42 (2003)
10. Jorns, O., Quirchmayr, G., Jung, O.: A privacy enhancing service architecture for ticket-based mobile applications. International Conference on Availability, Reliability and Security ARES 2007—The Dependability Conference, Vienna, Austria, April 10–13, 2007
11. Junglas, I.A., Spitzmüller, C.: A research model for studying privacy concerns pertaining to location-based services. In: Proceedings of the 38th Hawaii International Conference on System Sciences, 2005. HICSS '05. 03–06 Jan. 2005
12. Kölsch, T., Fritsch, L., Hohlweiss, M., Kesdogan, D.: Privacy for profitable location based services. In: Proceedings of the Second International Conference on Security in Pervasive Computing, Lecture Notes in Computer Science (LNCS 3450), pp. 164–179. Springer, Heidelberg (2005)
13. Lamport, L.: Password authentication with insecure communication. Commun. ACM 24(11), 770–772 (1981)
14. Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of applied cryptography. The CRC Press series on discrete mathematics and its applications. CRC, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA (1997)
15. Parlay X 2.0, The Parlay X 2.0 Specification, http://www.parlay.org/en/specifications/ (2006)
16. Price Blane, A.: The law is not enough: legislation and privacy enhancing technology for location-aware computing, workshop on location systems privacy and control, Mobile-HCI 2004, Glasgow, Scotland (2004)
17. Rodden, T., Friday, A., Müller, H., Dix, A.: A leightweight approach to managing privacy in location-based services, technical report equator-02-058. University of Nottingham and Lancaster University and University of Bristol (2002)
18. Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J.: A document format for expressing privacy preferences for location information, Internet-Draft, draft-ietf-geopriv-policy-08 (2006)
19. Treu, G., Küpper, A.: Datenschutzmechanismen für Ortsinformationen aus der Sicht zukünftiger Anwendungen, Tagungsband des zweiten GI/ITG KuVS Fachgesprächs über Ortsbezogene Anwendungen und Dienste, Informatikbericht 324, pp. 66–71. Fernuniversität Hagen, Stuttgart, Germany (2005)
20. Weiser, M.: The Computer for the twenty-first century, pp. 94–100. Scientific American, New York (1991)