Accountable Anonymous Service Usage in Mobile Communication Systems*

Levente Buttyán and Jean-Pierre Hubaux
Institute for computer Communications and Applications
Swiss Federal Institute of Technology
CH-1015 Lausanne, Switzerland
{Levente.Buttyan, Jean-Pierre.Hubaux}@epfl.ch

23rd June 1999

Abstract

We introduce a model that allows of anonymous yet accountable service usage in mobile communication systems. This model is based on the introduction of a new business role, called the customer care agency, and a ticket based mechanism for service access. We motivate the introduction of customer care agencies by analysing their role and emphasising their advantages. We introduce the general idea of ticket based service access, present a categorisation of ticket types and ticket acquisition models, and identify some possible attacks against ticket based systems. We illustrate how agencies and tickets work together by presenting a ticket based protocol between users, customer care agencies, and service providers. The protocol achieves authentication of the service provider to the user, establishment of a shared session key between the user and the service provider, and correct and undeniable charging. In addition, it provides revocable anonymity for users, which means that the identity of misbehaving users can be revealed.

1 Introduction

1.1 Background

Mobile communication systems allow their users to access a large set of traditional (e.g., voice communications) and contemporary (e.g., e-commerce) services without being tethered to one particular physical location. From a technology perspective, mobile communication systems have been made possible by two factors: advances in wireless communications and portable devices that are readily available on the market for decreasing costs. The former has resulted in a number of wireless access network technologies, such as, for instance, cellular telephone networks and wireless LANs. The latter is witnessed by high performance laptop computers, hand-held palmtop devices with considerable computing power, and portable telephone sets with increasing functionality. From a business perspective, mobile communication systems are

*EPFL SSC Technical Report No. SSC/1999/016

possible, because the mobility feature that they offer attracts many users. Mobile telephony, for instance, has been gaining more popularity among users than anybody predicted. In Europe, the number of mobile subscribers was 22 million in 1995 and is estimated to reach more than 110 million by 2000. In some countries (e.g., in Finland), the number of mobile subscriptions have already exceeded the figures for fixed telephone lines.

This success and popularity of mobile communication systems makes the provision of services to mobile users an attractive business area. Therefore, a great number and variety of service providers are expected to appear on the market in the near future. Services are usually categorised into two types, namely, basic communication services (e.g., traditional telephony and high speed data transfer) and value-added services (e.g., location adaptive information provision and video-on-demand). However, in this paper we do not make a distinction between these two types of services. We consider communication to be just one of the numerous services available to users. We distinguish only two basic roles: the user and the service provider.

1.2 Problems

Security in mobile communication systems has always been considered to be an important issue mainly because of the vulnerability of the air interface between the mobile terminal and the fixed network to various attacks. The Global System for Mobile Communications (GSM) [7], for instance, specifies mechanisms for user authentication as well as integrity and confidentiality protection of information exchanged between the mobile terminal and the fixed network. It provides limited privacy protection for users by hiding their real identities from eavesdroppers on the radio interface [8]. Other contemporary mobile communication systems (e.g., CDPD [2]) provide similar security services [4].

With the increasing use of mobile communication systems for security sensitive applications (e.g., e-commerce) that can be expected in the future, the provision of security services becomes even more important. However, there are at least two new challenges that future security architectures for mobile communication systems have to cope with:

- **Lack of trust.** The concept of security in today's mobile communication systems is based on a trust model that is not adequate for future mobile communication systems. Currently, in most cases, users are assumed to trust service providers to bill their service usage correctly and not to misuse user and service usage related information. With the rapidly growing number of service providers, most of which are new on the market and, thus, unknown to the users, this assumption is not justified anymore. Assuming that users and service providers mutually distrust each other seems to be more adequate in the future. This requires mechanisms that guarantee correct and undeniable billing and ensure anonymous yet accountable service usage.
- **Scalability.** Future mobile communication systems aim at offering access to *any service*, *anywhere*, at *any time*. The mechanisms of current mobile communication systems are not sufficiently scalable to be able to fulfil this promise. Traditional solutions for implementing user mobility rely on cross-domain authentication and roaming agreements. A user, when visiting a foreign domain and accessing a service there, has to authenticate himself to the foreign service provider with the help of his home domain agent. This

may involve a potentially time consuming authentication protocol over long distances. Furthermore, cross-domain authentication requires the foreign service provider to trust the home domain agent of the user. Today, this trust is based on roaming agreements between various service providers. With the rapidly growing number of service providers, however, roaming agreements are becoming infeasible and inefficient. New mechanisms are needed that do not require to contact the home domain of the user when accessing services in a foreign domain, neither business agreements between domains.

In brief, future mobile communication systems should guarantee higher level of security than current systems. This means that, besides confidentiality and integrity protection of messages exchanged between the user and the service provider, authentication of the user to the service provider, and anonymity to eavesdroppers on the air interface, future systems should also require authentication of the service provider to the user and guarantee higher level of privacy (e.g., anonymity of users to the service providers, location privacy and untraceability, etc.). In addition, correct and undeniable billing as well as scalability of mechanisms have to be ensured.

1.3 Approach

In this paper, we present a new approach that copes with the problems of lack of trust and scalability. This approach is based on the introduction of a new role, which we call *customer care agency*, and a *ticket based* mechanism for service access. The main idea is illustrated in Figure 1.

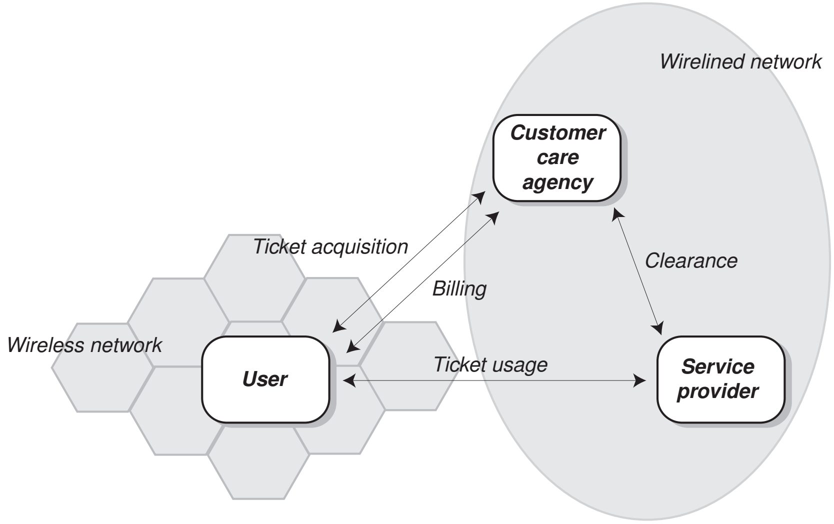

Figure 1: **Model**

In our model, each user is registered with a customer care agency. This agency issues tickets to its users, which they can use to access services anonymously. When requesting a service, the user is required to hand over an appropriate ticket, which provides an assurance to the service provider that it will be paid for the service provision. After checking the ticket, the service provider provides the requested service to the user. Later, in the clearance phase, the customer care agency pays for the services used by the user. The customer care agency, then, prepares a single bill for each user, which contains the charges for all the used services. An important feature of our model is that all the interactions between the user and the customer care agency, and between the service provider and the customer care agency can be made off-line.

This scenario is very much like an e-commerce setting. However, instead of buying products, in our model, users buy services from service providers. Nevertheless, the problems that we have to solve here are very similar to the problems that are encountered in e-commerce applications. It is no surprise that similar solutions suggest themselves. The customer care agency, for instance, can be considered as a response to the users' need for an organisation that helps them to cope with the complexity of the communications market. A similar phenomenon was the appearance of credit card organisations in the financial sector. We believe that there are many opportunities for exploiting e-commerce technologies in telecommunications. These opportunities hopefully enable greater user choice and greater competition, which lead to more user satisfaction and new forms of business.

1.4 Outline

We introduce our architecture in more detail in Section 2. Then, in the next two sections, we investigate the two most important features of our model. In Section 3, we analyse the role of customer care agencies, emphasise the advantages of their introduction, and explain why we believe that they can be better trusted by users than an arbitrary service provider. In Section 4, we introduce the general idea of ticket based service access, present a categorisation of ticket types and ticket acquisition models, and identify some possible attacks against ticket based systems. In Section 5, we illustrate how agencies and tickets work together by presenting a ticket based protocol between users, customer care agencies, and service providers. We compare our solution to other approaches to the same problem in Section 6. Finally, in Section 7, we conclude the paper.

2 Model

Our model is illustrated in Figure 1. It consists of three roles (the user, the service provider, and the customer care agency) and a protocol with several sub-protocols (ticket acquisition, ticket usage, clearance, and billing) between these roles. We assume that each user is registered with a customer care agency. The user obtains tickets by running the ticket acquisition protocol with his customer care agency. These tickets can be used to access services anonymously. In the ticket usage protocol, the user presents an appropriate ticket to the service provider, which can verify the validity of the ticket and the legitimacy of the user to use it. While the user's identity is not revealed in this protocol, the service provider authenticates itself to the user. If the verification of the ticket is successful, then the service provider provides the service to the user according to the conditions on the ticket. Used tickets are stored by the service provider and later, in the clearance protocol, presented to the customer care agency of the user. Based on the received tickets, the customer care agency pays for all the service usages of its users and, then, prepares a single bill for each user, which contains the charges for all the used services. The exact form of the clearance (payment to the service provider) and billing (payment to the customer care agency) protocols are not specified in our model. They can be based on electronic payment protocols or business agreements between the parties. We do not consider this incompleteness of our approach to be a drawback, but an advantage, which allows of modularity, flexibility, evolvability, and interoperability. An important feature of our model is that all the interactions between the user and the customer care agency, and between the service provider and the customer care agency can be made off-line.

The problems of lack of trust and scalability are addressed in the following ways:

- **Trust.** Tickets provide anonymous access to services for users, therefore, users do not need to trust service providers to handle user and service usage related information carefully. On the other hand, service providers authenticate themselves to accessing users, thus, the user can be sure that the service is provided by the selected service provider. Service providers can verify the validity of the tickets and check if they were used by their legitimate users. This gives sufficient assurance for service providers that they will be paid for the service provision. Furthermore, the correct charging and undeniability of service usage can also be guaranteed by a simple protocol. If necessary, anonymity can be revoked and users can be held accountable for their malicious behaviour; this would, however, happen only in special circumstances and typically under judicial supervision.

- **Scalability.** Instead of contacting the home domain agent of the accessing user, in our model, the service provider has to verify only the ticket and the legitimacy of the user to use it. None of these require to run long-distance protocols with the customer care agency of the user. In most of the cases, the ticket will be acquired by the user from the customer care agency before roaming into the foreign domain. Thus, ticket acquisition usually does not require long-distance protocols neither. Regarding business agreements, they are not needed anymore, although, they might be advantageous in facilitating clearance of payment between customer care agencies and service providers. However, the number of customer care agencies can be kept small, which would reduce the number of business agreements between the parties.

Besides solving the trust and scalability problems, our model has the following additional advantages:

- **Modularity and evolvability.** Ticket acquisition and usage, billing of users, and clearance of payments are clearly separated parts in our model. This modularity makes it easy to replace one part without serious effects on the other parts. Replacement might be necessary because of evolution of algorithms and technology. Furthermore, the clearance protocol between the service provider and the customer care agency, and the billing protocol between the customer care agency and the user are not fully specified and allows of the integration of various payment mechanisms.

- **Efficiency.** Users can leverage from the fact that they have an agent (the customer care agency) located within the wirelined network. They can, for instance, delegate tasks that demand too much resources and/or communications to this agent. Our protocols, for instance, are optimised in a way that as much computations and communications as possible is performed by the customer care agency on behalf of the mobile user. Furthermore, the mobile user can be disconnected while the customer care agency works on a complex task and obtain the result at the next time he connects again. This is a very efficient use of bandwidth, which is considered to be expensive in wireless networks.

- **Gradual deployment.** Although the customer care agency is a distinct role in our model, we do not exclude the possibility that it is played by a telecommunication service provider. The concept of home domain is well established in current mobile communication systems, and the operator of the home network of the user can easily play the role of the customer care agency. In this case, the deployment of our model does not require the establishment of a brand new infrastructure. In the future, however, we expect that the customer care agency role will be played by other organisations too.

3 The customer care agency

3.1 Role

Customer care agencies take care of the interests of their users. They issue tickets to their users that let them access services anonymously and handle payments on behalf of their users. Thus, customer care organisations play an important role in the protection of the privacy of their users. Besides supporting user privacy, the main advantages of having customer care agencies are the following:

- **Separation of roles.** In current mobile communication systems, billing of users is performed by telecommunication network operators, although, the main role of these operators is, indeed, the provision of communication services. The strong bundling between the network access and the money collection functions are a legacy of the classical wirelined telephone model, where a given terminal is physically attached to a local switch operated by a given network operator. As soon as the terminal becomes mobile and roams across the domains of different operators, this static relationship disappears. In that case, there is no particular reason anymore to have one specific network operator performing billing and authentication functions for a given user. Therefore, in our model, billing and authentication are *factored out* into customer care agencies, which can be viewed as special service providers that are specialised on these functions.

- **Customer care.** The complexity of communication systems are going to become such high that residential end-users as well as small to medium size enterprises will not be in a position to take care of optimising the selection of service providers, protecting their privacy, defending their rights, etc. Therefore, they will need a special organisation, which helps them to find their way in this complex world. Customer care agencies, in our model, can provide this help. They can cope with the complexity of the communication market and negotiate optimal deals from the providers on behalf of their users.

To some extent, the customer care agencies are going to appear as a response to the quickly growing number of network operators and service providers. A very similar phenomenon occurred in the financial sector, where the credit card organisations appeared as a response to the growing number of banks. In the same way as it became impossible to conclude direct deals between all consumers, banks, and shops, it is going to become impossible to conclude direct deals between end users, network operators, and service providers. It is noteworthy that, in fact, the credit card organisations have an extremely high responsibility in the protection of the consumers' privacy. It would be no surprise if they would demonstrate interest in entering the business of customer care.

Customer care agencies are profit-oriented organisations. They must obtain a licence from a national or international authority. Within well-defined rules, they compete with each other and try to maximise user satisfaction. Because of their pivotal role in guaranteeing optimal communication deals as well as privacy, customer care agencies would be under the close supervision of consumer organisations.

3.2 Trust

We should note that, in our model, the user is required to trust his customer care agency, because it has access to private information about its users and performs tasks on behalf of its users that require the users to have high confidence in it. This trust, however, can be based on the following [11]:

- **Specialisation.** Customer care agencies would be specialised on privacy protection and billing and, thus, more competent in the provision of these services than information service providers and network operators.
- **Control.** The number of customer care agencies would be kept small, which makes supervision and law enforcement an efficient approach to the control of their operation. They would be subject to regular and thorough control by external appraisal organisations. The result of these controls would be made publicly available to raise users' confidence and obtain a better position in the market (similar to the approach for quality assurance in ISO-9000).
- **Reputation.** We assume that customer care agencies would be major corporations, which have the necessary resources to build a good reputation and the incentive to protect it.
- **Separation of concern.** Customer care agencies would have nothing to gain by not accomplishing their tasks. Indeed, their business would be to take care of their users, which includes the protection of their privacy, handling payments, etc, therefore, it would be in their interest to perform these functions correctly.

4 Ticket based service access

In this section, we discuss the general idea of ticket based service access. This is independent of the concept of customer care agencies, therefore, we leave the assumption of having such an agency in our model. We return to this assumption in the next section, in which we illustrate how customer care agencies and tickets work together by presenting a ticket based protocol between users, customer care agencies, and service providers.

4.1 Tickets

Using tickets to access various services is a well established concept in every day life. We use tickets, for instance, to travel on a train or bus, to enter to a cinema or museum, etc. Intuitively, a ticket is a piece of information that represents the rights of a certain user to access a certain service provided by a certain service provider. A flight ticket, for instance, can be used by its legitimate holder (user) to fly from one place to another (service) with the airplane of an air company (service provider). A ticket may also have associated with it a number of conditions (e.g., validity period).

There is nothing to prevent us to apply the concept of ticket based service access in the context of communication systems. Tickets can be used to access basic communication services (wireless and wireline), as well as value-added services (e.g., video-on-demand). The meaning of a ticket is the same in this context too, namely, a piece of information that represents rights. The physical realization of a ticket, however, is different: it is realized in a pure electronic form (i.e., as a string of bits).

The main advantages of using tickets for accessing services are the following:

- **Flexibility.** Users can easily construct personalised service profiles by buying the appropriate set of tickets. They do not have to engage into long term contractual relationships with service providers. Instead, they can choose services as they need them and in a way that matches their personal requirements.
- **Scalability.** The ticket can contain all the necessary information for the service provider to decide if it should provide the service or not. Thus, there is no need to run long-distance protocols with some trusted agent of the accessing user in order to perform authentication. This makes ticket based service access an appealing approach in mobile communications where users roam and contact service providers in foreign (and potentially distant) domains.
- **Privacy.** A ticket based mechanism, together with a trusted agent, which issues tickets and handles payments on behalf of users, can protect the privacy of users efficiently. The user only has to demonstrate that he is a legitimate holder of the ticket, and he does not necessarily have to reveal his real identity. Thus, no private information is available to service providers.

4.2 Types

Although, in the most specific case, a ticket binds a given user, a given service, and a given service provider together, this is not necessarily always the case. Consider, for instance, a bus ticket, which usually does not specify who can use it (i.e., the user), or a travel card, which may not restrict the means of transport (i.e., the service). Based on this observation, we can identify eight types of tickets. This is illustrated in Table 1, where $\times$ means that the entity, which labels the corresponding row of the table, is bound by the ticket, while $-$ means that it is not.

A ticket of type t_0, for instance, does not restrict the service, for which it can be used, the service provider, which accepts it, and the user, who can use it. This is much like cash

	Types							
	t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7
user	$-$	$-$	$-$	$-$	$\times$	$\times$	$\times$	$\times$
provider	$-$	$-$	$\times$	$\times$	$-$	$-$	$\times$	$\times$
service	$-$	$\times$	$-$	$\times$	$-$	$\times$	$-$	$\times$

Table 1: Ticket types

in real life. The other extreme is a ticket of type t_7, which can only be used by a given user, for a given service, provided by a given service provider. An example of this type is the flight ticket mentioned before.

Tickets can be further categorised according to the type of payment and their validity. With regard to payment, a ticket can be:

- **Pre-paid.** The ticket is paid at acquisition time before usage.
- **Post-paid.** The ticket is paid only after it has been used.

With regard to its validity, a ticket can be:

- **n-times ticket.** A ticket of this type can be used at most n times.
- **Subscription.** This type of tickets can be used any times within a given validity period.

4.3 Acquisition models

Ticket acquisition can follow one of the following three basic models or some combination of them:

- **Outlet model.** In this model, the user acquires the ticket directly from the service provider. The advantage of this approach is that ticket acquisition does not require additional infrastructure. The disadvantage is that the acquisition of tickets may require users to run expensive and complicated protocols to find the optimal service provider, which offers the best price, the best quality, or the optimal combination of the two.
- **Kiosk model.** Tickets of various service providers are sold by a special service provider called the kiosk. This model overcomes some of the disadvantages of the outlet model: users do not have to contact each service provider if they need a ticket, but they can contact the kiosk, where information about the offers of several service providers is available and selection of the optimal one is easier. But still, users have to make the decision themselves, which requires resources. Another disadvantage is that this model requires infrastructure to be built up (the kiosks).
- **Agency model.** In this model, the tickets are chased up and bought by agencies that act on behalf of users. The main advantage of this approach is that users can obtain

the best tickets in an easy way by allowing the agency to contact the service providers and run expensive protocols in order to find the optimal offer. The disadvantage of this model is that it requires infrastructure (the agencies). Furthermore, agencies are considerably more complex entities than kiosks and they possible require to be paid by the users in return for their services.

An additional disadvantage of the agency model is that agencies may need to contact a very large number of service providers when searching for tickets on behalf of users. In order to overcome this problem, a combination of the kiosk and the agency model can be used, in which agencies buy tickets from kiosks.

4.4 Attacks

The main problem with the pure electronic representation of tickets is that, without cryptographic protection, it becomes easy to fabricate, modify, and copy (and then use or re-use) them. Fabrication, modification, and illegitimate use or re-use are typical attacks, which can be mounted by outside attackers or malicious users of the system, with the hope of using services without paying for them.

Service providers can also try to subvert the ticket system aiming at getting paid without providing the service. They may try to get the same ticket sold twice but accept it only once or not accept it at all. These are, however, less important attacks, since we assume that the service provider would loose more (its reputation) than it would gain, especially if the tickets have low value. Therefore, the service provider is interested to provide the service and behave correctly. Nevertheless, our protocols presented in Section 5 prevent or detect some of these and similar misbehaviours of service providers.

5 Protocol

In this section, we demonstrate the concepts of customer care agency and ticket based service access by a protocol that relies on them. The protocol, which we present in the sequel, uses *one-time use*, *post-paid* tickets of type t_4. Protocols for other ticket types are also interesting; we leave the development of them for future work. Tickets are acquired following the agency model for ticket acquisition, since it fits naturally in our model (i.e., tickets are obtained from the customer care agency).

Tickets of type t_4 are particularly interesting because they do not specify the service, for which they can be used, neither the service provider, which accepts them. Therefore, they can be used in a flexible and ad hoc manner. In general, the user does not know in advance in which distant domains he will roam and which services he will request there. t_4 tickets solve the problem: the user can obtain a couple of them once and he can use them later with any service provider for any service.

t_4 tickets, on the other hand, restrict the user, who can use them. This, however, does not mean that anonymity is lost. In our protocol, for instance, the user is required to demonstrate knowledge of a private parameter, which corresponds to the ticket and which is known only to the legitimate holder of the ticket. This demonstration does not reveal the identity of the user.

Since tickets are post-paid, their value can be determined dynamically at service access time. This gives an additional level of flexibility to users. But it also requires some extra information to be exchanged between the user and the service provider. This means that the service provider has to send its tariff for the service to the user, and the user has to commit to this tariff.

The protocol presented here, has been developed for the access to stream oriented services (e.g., video-on-demand). In order to guarantee correct and undeniable charging for such services, we need an additional mechanism. The usual solution, in such cases, is based on a "tick" protocol [10] between the user and the service provider, in which the user periodically sends "ticks" to the service provider as an acknowledgement of received service and a request for further service provision. This standard solution has been proposed by several authors [5, 6, 13]. We integrated the initialisation of the "tick" protocol in our ticket based protocol.

5.1 Notation

K_{xy}	A key shared by principal X and Y.
K_x^+, K_x^-	A public and a private key of principal X.
dh_x^+, dh_x^-	A public and a private Diffie-Hellman key exchange parameter.
$\{M\}_K$	A message M encrypted with the key K.
$\sigma_{K_x^-}(M)$	A signature on message M generated with the private key K_x^-.
$h(M)$	The cryptographic hash value of a message M.
$X \to Y:\ M$	A message M sent by principal X to principal Y.

5.2 Ticket acquisition

1. The user U requests a ticket from the customer care agency A:

$$U \to A: \quad (Uid,\ r_0)$$

   Uid is the identity of the user and r_0 is a freshly generated random number.

2. The agency constructs the ticket:

$$T = (sn,\ c_n,\ dh_u^+,\ K_u^+,\ Aid,\ \sigma_{K_a^-}(sn, c_n, dh_u^+, K_u^+))$$

   The ticket contains a serial number sn, a freshly generated public Diffie-Hellman key exchange parameter dh_u^+, a freshly generated public signature verification key K_u^+, and the initial parameter c_n for the "tick" protocol. $c_n = g^{(n)}(c_0)$, where g is a one-way function, $g^{(k)}$ denotes the k-th iteration of g, and c_0 is a freshly generated random seed. The ticket also contains the digital signature of the customer care agency A, and some information about the agency. This information includes at least the identity Aid of the agency, but possibly also its public signature verification key and a digital certificate that binds the key to the identity (for simplicity, we did not include these in the protocol presented here).

3. The agency sends the ticket to the user together with the private parameters c_0, dh_u^-, and K_u^-:

$$A \rightarrow U: \quad \{T,\ c_0,\ dh_u^-,\ K_u^-,\ r_0\}_{K_{ua}}$$

The message is encrypted with the key K_{ua} using a symmetric encryption algorithm. K_{ua} is shared by the user U and the agency A; no other entity knows this key. It is established at the time when the user registers with the agency. This encryption provides the necessary confidentiality for the communication of the private parameters, which should be known only to the user. The presence of r_0 proves the freshness of the ticket to the user. The agency keeps a copy of the ticket in an internal database for later use.

5.3 Ticket usage (initialisation)

1. The user U obtains an authentic copy of the public Diffie-Hellman key exchange parameter dh_s^+ of the service provider S. This parameter can be acquired in several ways. If the user knows in advance which service provider he wants to contact, then the public key exchange parameter of this service provider can be obtained in an off-line fashion well before the service usage. Another way to get it is to use a local directory service. The mobile user can, for instance, be in a foreign domain and may want to access a service there. He can use a local directory service to download a digital certificate containing the required key exchange parameter of the service provider. Alternatively, if the service provider is a cellular network operator, then it can broadcast its digital certificate continuously via a broadcast control channel [12].

2. The user computes a session key k using his private Diffie-Hellman key exchange parameter dh_u^- and the service provider's public parameter dh_s^+.

$$k = f_u(dh_u^-, dh_s^+)$$

This key is used to authenticate the service provider and to encrypt and decrypt messages to and from the service provider (e.g., service contents).

3. The user sends a service request to the service provider:

$$U \rightarrow S: \quad (T,\ r_1)$$

The request contains the ticket T and a freshly generated random number r_1.

4. The service provider computes the session key k, using its own private Diffie-Hellman key exchange parameter dh_s^- and the public parameter dh_u^+ of the user, which is in the ticket.

$$k = f_s(dh_s^-, dh_u^+)$$

The authenticity of dh_u^+ is guaranteed by the digital signature of the agency on the ticket. In order to verify this signature, the service provider needs the public signature verification key of the agency, which it can obtain from a public directory. k is the same key as the one computed by the user, thus, it can be used to encrypt messages to the user (e.g., service contents).

5. The service provider authenticates itself and communicates the tariff t for the service by sending the following message to the user:

$$S \to U: \quad (t,\ h(k,t,r_1),\ r_2)$$

r_2 is a freshly generated random number and $h(k,t,r_1)$ is the hash value of the concatenation of k, t, and r_1.

6. The user checks the hash value $h(k,t,r_1)$. The presence of k guarantees authenticity and the presence of r_1 proves freshness. Thus, successful verification of the hash value ensures the user that he communicates with the right service provider, who knows the private Diffie-Hellman parameter dh_s^- that corresponds to dh_s^+.

7. The user confirms the service request and commits to the tariff by signing the serial number sn of the ticket T together with the tariff t and the random number r_2. The signature is sent to the service provider:

$$U \to S: \quad \sigma_{K_u^-}(sn,t,r_2)$$

8. The service provider verifies the signature and keeps it for later usage.

5.4 Ticket usage (service provision)

The following steps are repeated several times (as it is described in [10]). We assume that the last "tick" sent by the user is c_l. The last "tick" is always stored by the service provider.

1. The service provider sends a request for d ticks.

2. The user computes $c_{l-d} = g^{(l-d)}(c_0)$, and sends it to the service provider.

3. The service provider checks the "tick" by computing $g^{(d)}(c_{l-d})$. If the result is c_l, then it provides the next part of the service according to the tariff (e.g., next x bytes of data).

5.5 Clearance and billing of the user

1. The service provider sends the proof of service usage to the customer care agency:

$$S \to A: \quad (sn,\ t,\ r_2,\ \sigma_{K_u^-}(sn,t,r_2),\ c_l,\ Sid,\ \sigma_{K_s^-}(sn,t,r_2,\sigma_{K_u^-}(sn,t,r_2),c_l))$$

This contains the serial number sn of the ticket used by the user, the tariff t, the random number r_2, the commitment of the user $\sigma_{K_u^-}(sn,t,r_2)$, and c_l, which proves that the user sent $n-l$ "ticks" to the service provider. The message is signed by the service provider.

2. The customer care agency, after checking the digital signature of the service provider, verifies that sn is a valid serial number of a ticket issued by itself and that no request with the serial number sn arrived before. If this is the case, then the service provider and the customer care agency run a payment protocol, in which the agency pays for the service. The agency stores the proof of service usage for later verification purposes.

3. Finally, based on the proofs of service usage received from the service providers, the customer care agency constructs an aggregated bill for the user.

5.6 Evaluation

Outside attackers cannot fabricate and modify tickets, because they cannot generate a valid signature in the name of the customer care agency. Although an attacker can eavesdrop a valid ticket, he cannot use it later, because he cannot generate the signature required for the commitment to the tariff in the ticket usage phase. In order to generate this signature, he has to know the private signature generation key, which is sent to the legitimate user of the ticket in encrypted form. Thus it is known only to the user and the customer care agency, which is a trusted entity.

Users cannot fabricate and modify tickets neither, because of similar reasons why outside attackers cannot do that. They can try to re-use a previously used ticket, but they will be caught by the customer care agency. The user can receive the service only if he commits to the tariff by signing the serial number sn of the ticket, the tariff t, and a random number. This commitment is sent by the service provider to the customer care agency in the proof of service usage. If the same ticket is used twice, then the customer care agency receives two proofs of service usage with the same serial number sn. Furthermore, since the service providers store commitments, if the user tries to use the same ticket twice with the same service provider, then the service provider can also discover the misbehaviour.

A service provider can deny the provision of service after having accepted the ticket and the commitment of the user. However, it would not gain too much, because the amount of money that it can claim depends on the last "tick" received from the user. If the service provider denies the service provision, then the user does not send more "ticks". Thus, all the service provider can gain is an amount that corresponds to the number of the last requested "ticks", which is possibly not too high. Furthermore, "ticks" cannot be forged because of the one-way property of the function g.

6 Discussion

It should be noted that some embryonic form of a customer care function, similar to the one we described in this paper, already exists today with the access network operators. In the US telephone network, for instance, the local network operator can bill the user for all his phone calls and then transfer the appropriate amounts to the long distance carrier(s). Furthermore, in the videotex (and notably in the French minitel), all payments from the users to the information service providers flow through the network operator. Because the terminal is not attached to a given network anymore, we strongly believe in the separation of the customer care function from the connectivity provision. This separation brings interesting side-effects. For example, one of the problems of current cellular networks is that the services do not behave in the same way according to whether the end user is located in his home network or is roaming [3]. If the customer care concept is fully implemented, then the distinction between home and visited networks disappears and, thus, the behaviour of the services becomes independent of the access network.

The problem of anonymous yet accountable service usage in mobile communication systems is addressed in [1]. The authors propose the use of an anonymous tokening system to solve this problem. In this solution, the home network of the user provides tokens to the user, which are stored and then used as the user receives service from the service provider. The number of tokens used indicates how much to bill the user. In order to provide anonymity, the tokens are blinded and paid at acquisition time. When used, the validity of a token can be checked, but not to whom it was issued. When the service provider redeems the token, it can be validated by the home network. Since the tokens have already been paid before, the origin of the token is not important.

An approach that is very similar to the one presented in this paper is proposed in [5, 6] for the third generation mobile system (UMTS). In this solution, the user obtains tokens from the UMTS service provider, who acts as a broker. The tokens are then handed off by the user to the value-added service provider as a proof of his credit-worthiness. The settlement between the value-added service provider and the broker is then accomplished off-line. The UMTS service provider will collect the billing information from all the value-added service providers accessed by a given user and integrate them in a single bill addressed to the user. This mechanism is a very significant improvement over the ones prevailing in the second generation mobile systems. However, it has the weakness of not providing anonymity to the users.

Another similar approach for ticket based service access is described in [9]. In this proposal, tickets are pre-paid and can only be used with the service provider that issued them (according to our categorisation, tickets are type t_7 and acquired following the outlet model). Anonymity can be provided for all services for which it is deemed appropriate.

It has to be noted that these solutions as well as our one require to have a common protocol and ticket format for all users and all service providers. However, there is little probability that such a common mechanisms can be deployed world-wide. For instance, even if the previously mentioned UMTS solution is deployed continent-wide in Europe, it might not work for transactions in which the user is located in Europe and the service provider in the US and vice-versa. In addition, it seems to be dangerous to have a single worldwide security scheme between users and service providers. This scheme would be the least common denominator of available security technologies; it would have to be hardwired in end-systems, becoming a potential stumbling block for the acceptance of future security technology.

A solution to this problem can be based on the download of software containing new security mechanisms. However, downloading software that performs security functions is dangerous, because it can contain back doors, which practically cannot be discovered by ordinary users. These back doors can be exploited by those who know them to subvert the system. The customer care agency of our model can help to solve many of the problems related to this issue. Let us assume, for instance, that a service provider wants to move to another, more secure ticket mechanism. It will then get in touch with all customer care agencies with which it has a business agreement to ask for this upgrade. The customer care agency will then check this new mechanism, sign it, and download it into all terminals it is taking care of. For each terminal, this operation can, for instance, be performed at the next time the terminal asks for new tickets. Assuming that the customer care agency can reliably verify the code of the new ticket mechanism is more realistic than assuming the same about users because the customer care agency can have the necessary resources and competence to perform such verifications. Then, the users only need to check the signature of the agency on the code.

7 Conclusion

Mobile communication systems are becoming extremely popular, which makes the provision of services to mobile users an attractive business area. This can be regarded as a special form of e-commerce, where users buy services instead of products from service providers via the network. There are many opportunities for exploiting e-commerce technologies in this setting, which allows users to choose their providers in a more flexible way and stimulate stronger competition among service providers. This can lead to more user satisfaction and new forms of business.

In order to make this feasible, we have identified two conditions that have to be fulfilled. First, there must be a customer care organisation that assists the user in his usage of the network, in optimising his requests, and in protecting his privacy. Second, a homogeneous token-based or ticket-based mechanism must be implemented allowing the user to remunerate the service providers, with the assistance of the customer care organisation.

In this paper, we proposed a model that fulfils these conditions. Our model is based on the introduction of customer care agencies and a ticket based mechanism for service access. The customer care agency is a special service provider that helps the user to choose service providers, handles payments on behalf of the user, and takes care of protecting the user's privacy. This is achieved by issuing tickets to the user that can be used to access services anonymously yet in an accountable way. Tickets provide a flexible and scalable mechanism for users for accessing services; their usage in mobile communication systems is particularly advantageous. The characteristic features of our design are modularity, evolvability, interoperabilty, efficient use of bandwidth, and the possibility of gradual deployment.

References

[1] B. Askwith, M. Merabti, Q. Shi, and K. Whiteley, Achieving User Privacy in Mobile Networks, 13th Annual Computer Security Applications Conference, 1997.

[2] CDPD Forum, Cellular Digital Packet Data System Specification, Release 1.1, January 1995.

[3] ETSI TS 101 044, Customized Application for Mobile Network Enhanced Logic, Stage 2, November 1997.

[4] Y. Frankel, A. Herzberg, P. A. Karger, H. Krawczyk, C. A. Kunzinger, and M. Yung, Security Issues in a CDPD Wireless Network, *IEEE Personal Communications*, August 1995.

[5] G. Horn and B. Preneel, Authentication and Payment in Future Mobile Systems, ESORICS, 1998.

[6] K. M. Martin, B. Preneel, C. J. Mitchell, H. J. Hitz, A. Poliakova, and P. Howard, Secure Billing for Mobile Information Services in UMTS, IS&N, 1998.

[7] A. Mehrotra, GSM System Engineering, Norwood, Artech House, 1997.

[8] A. Mehrotra and L. S. Golding, Mobility and Security Management in the GSM System and Some Proposed Future Improvements, *Proceedings of the IEEE*, 86(7), July 1998.

[9] B. Patel and J. Crowcroft, Ticket Based Service Access for the Mobile User, Mobicom, 1997.

[10] T. P. Pedersen, Electronic Payments of Small Amounts, DAIMI PB-495, Computer Science Department, Aarhus University, August 1995.

[11] U. Wilhelm, S. Staamann, and L. Buttyán, On the Problem of Trust in Mobile Agent Systems, NDSS, 1998.

[12] Y. Zheng, An Authentication and Security Protocol for Mobile Computing, IFIP World Conference on Mobile Communications, 1996.

[13] J. Zhou and K-Y. Lam, Undeniable Billing in Mobile Communication, Mobicom, 1998.