Accountable Anonymous Access to Services 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

Abstract

We introduce a model that allows anonymous yet accountable access to services 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 introduce the general idea of ticket based service access, and present a categorisation of ticket types and ticket acquisition models. We analyse the role of customer care agencies and emphasise their advantages.

1 Introduction

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. Examples of mobile communication systems include cellular telephone networks and wireless LANs. The mobility feature offered by these systems attracts many users[1]. This makes the provision of services to mobile users a promising 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. 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.

1.1 Problems

With the increasing use of mobile communication systems in a variety of applications (also including security sensitive applications, such as e-commerce) the provision of *security guarantees* to service providers and users (also including the protection of user privacy) is becoming an important issue. In addition, 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 inadequate for future mobile communication systems. Currently, it is assumed that users trust the service providers to charge for services used correctly and not to reveal or misuse any 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. To assume that users and service providers mutually distrust each other would be more appropriate for the future. This requires mechanisms that guarantee correct and undeniable charging and ensure anonymous yet accountable service access.
- **Scalability.** Future mobile communication systems aim at offering access to *any service*, *anywhere*, at *any time*. However, the mechanisms of current mobile communication systems may not be sufficiently scalable to be able to fulfil this promise. Let us consider, for instance, traditional solutions for implementing user mobility. They 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.

 Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems (SRDS'99). Workshop on Electronic Commerce (WELCOM).

[1] Mobile telephony, for instance, is gaining more popularity among users than anyone ever predicted. In Western Europe, the number of mobile subscribers exceeded 110 million in June 1999, while it was less than 22 million in 1995.

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 the foreign domain and the home domain. With the rapidly growing number of service providers, however, roaming agreements are becoming unfeasible 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.

1.2 Approach

In this paper, we present a new approach for controlling access to services that copes with the problems of lack of trust and scalability. This approach is based on the introduction of a new business role, which we call *customer care agency*, and a *ticket based* mechanism for service access (Figure 1).

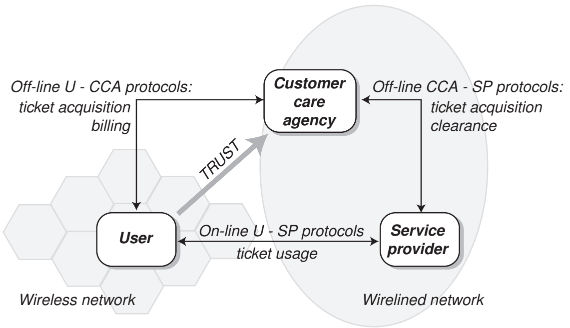

Figure 1. Model

Our model is very similar to the typical model of e-commerce. However, instead of buying products, in our model, users buy services from service providers. Nevertheless, our problems are very similar to those encountered in e-commerce applications. It is no surprise that similar solutions suggest themselves. We believe that there are many opportunities for exploiting e-commerce technologies in telecommunications. We hope that these opportunities will enable greater competition and more user choices, which will lead to greater user satisfaction and new businesses.

1.3 Outline

We introduce the general idea of ticket based service access, and present a categorisation of ticket types and ticket acquisition models in Section 2. Then, we introduce our model in more detail in Section 3. In Section 4, we investigate the key component of the model: the customer care agency. We analyse its role, emphasise its advantages, and explain why we believe that it can be better trusted by users than an arbitrary service provider. We compare our solution to other approaches to the same problem in Section 5. Finally, in Section 6, we conclude the paper.

2 Ticket based service access

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 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 air-plane 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, specifically, 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 as best matches their personal requirements.
- **Scalability.** For the service provider to decide if it should provide the service or not, the ticket can contain all the necessary information. 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 that issues or acquires tickets and handles payments on behalf of users, can efficiently protect the privacy of users. The user only has to demonstrate that he is a legitimate holder of the ticket, and

he does not necessarily have to reveal his true identity. Thus, no private information is available to service providers.

The main problem with the pure electronic representation of tickets is that, without cryptographic protection, it becomes easy to fabricate, modify, and copy them. Fabrication, modification, and illegitimate use or re-use of copied tickets 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. These problems are similar to the problems that are encountered in electronic payment systems and we can easily borrow mechanisms from that domain to address them. Space limitations do not allow us to review these mechanisms here. For a comprehensive survey of electronic payment systems, we refer to [6].

2.1 Ticket types

In the most specific case, a ticket binds a given user and a given service provider together. However, 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). Based on this observation, we can identify four types of tickets depending on the bound entities. 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.

	Types			
	t_0	t_1	t_2	t_3
user	$-$	$-$	$\times$	$\times$
provider	$-$	$\times$	$-$	$\times$

Table 1. Ticket types

A ticket of type t_0, for instance, does not restrict the service provider, which accepts it and the user, who can use it. This is much like cash in real life. The other extreme is a ticket of type t_3, which can only be used by a given user, for a 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 time of payment and their validity. With regard to the time of payment, tickets can be paid upon acquisition (*pre-paid*) or after they have been used (*post-paid*). With regard to their validity, tickets can be used at most n times (*n-times tickets*) or any times within a given validity period (*subscriptions*).

2.2 Ticket 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 a 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 could require to be paid by the users in return for their services.

3 Model

Our model is illustrated in Figure 1. It consists of three roles (the user, the service provider, and the customer care agency) and various protocols (ticket acquisition, ticket usage, billing, and clearance.) between these roles. Due to space limitations, we omit the detailed description of protocols and give a high level view of the system. For more details, we refer to [2].

In our model, access decision to services is based on tickets. When requesting a service, the user is required to hand over an appropriate ticket, which provides assurance to the service provider that it has been (in case of pre-paid tickets) or will be (in case of post-paid tickets) paid for the service provision. After checking the ticket, the service provider provides the requested service to the user according to the conditions on the ticket.

Tickets are anonymous (i.e., type t_0 or t_1), but they contain some information that allows the service provider to verify the legitimacy of the user to use it[2]. While the identity of the user is not revealed to the service provider, we require the service provider to authenticate itself to the user.

We assume, that each user is registered with a customer care agency, which he trusts and from which he obtains the tickets that are required to access services. Depending on its type, the ticket can be issued by the customer care agency (type t_0) or by a service provider (type t_1). If the ticket is issued by a service provider, then the customer care agency obtains it from the service provider and forwards it to the user (i.e., ticket acquisition follows the agency model).

All payments are handled by the customer care agency on behalf of the user, who receives a single bill from the agency, which contains the charges for all the used services. Used post-paid tickets are stored by the service provider and (at some later time) presented to the customer care agency, which settles the payment with the service provider. 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 (i.e., they do not necessarily take place at service access time).

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 access 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 have been or will be paid for the service provision. Furthermore, correct charging and undeniability of service usage can also be guaranteed by integrating an appropriate ticket slicing mechanism, similar to micropayment schemes [8], into the ticket usage protocol (see [2] for details). If necessary, anonymity can be revoked and users can be held accountable for their malicious behaviour. This is possible, because the customer care agency can always link a ticket to the user who obtained it.

- **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 either. Regarding business agreements, they are not needed anymore, although, they might be advantageous in facilitating 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 an 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 thus allowing for 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 many resources and/or communications to this agent. The protocols can be optimised in a way that as many computations and communications as possible are 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. This is a very efficient use of bandwidth, which is considered to be expensive in wireless networks.

- **Gradual deployment.** Although the customer care agency has a distinct role in our model, we do not exclude the possibility that it can be 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

[2] For instance, the ticket may contain a public key and the user may be required to demonstrate knowledge of the corresponding private key. But the public key is bound to the ticket (by the signature of the issuer of the ticket) and not to the identity of the user.

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.

4 The customer care agency

The complexity of communication systems will become so 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 that helps them to find their way in this complex world. Customer care agencies, in our model, are meant to provide this help. They can cope with the complexity of the communication market, and they take care of the interests of their users. They negotiate optimal deals from the providers and handle payments on behalf of their users, and obtain or issue tickets to their users that let them access services anonymously.

To some extent, the customer care agencies will 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 will 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 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 augment 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.

We note that in current mobile communication systems billing 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 this case, there is no particular reason anymore to have one specific network operator performing billing (and other customer care functions) for a given user. Therefore, in our model, customer care functions are *factored out* into customer care agencies and separated from service provision.

This separation brings interesting side-effects. For instance, 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.

4.1 Trust in the customer care agency

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 [9]:

- **Specialisation.** Customer care agencies would be specialised on privacy protection and billing and, thus, more competent in the provision of these services than (especially small) service providers.

- **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.

5 Related work

The problem of anonymous yet accountable service access in mobile communication systems is addressed in [1].

The authors propose the use of an anonymous tokening system, similar to anonymous digital cash systems, to solve this problem. Tokens are issued by the home network of the user, which plays a role similar to the one played by the customer care agency in our model. In order to provide anonymity, the tokens are blinded and paid at acquisition time. The validity of a token can be checked by the service provider (when the token is used by the user) as well as by the home network (when the service provider redeems the token) but not to whom it was issued. Thus, this solution provides user anonymity with respect to the home network, too, at the expense of a more complex protocol between the user and the home network. On the other hand, this solution does not allow service providers to issue tokens. Although tokens issued by a service provider are not as flexible (they can only be used with the issuing provider), they might have some other advantages. For instance, they can be interpreted as reservations (of resources). Our model is more general in the sense that it allows for both type of tokens (tickets).

Another approach is proposed in [4, 5] for the third generation mobile system (UMTS). In this solution, the user generates tokens and hands them off to the service provider as a proof of service usage. The service provider then contacts the UMTS service provider of the user, which plays a role similar to our customer care agency role, and the settlement is accomplished off-line. The UMTS service provider collects the billing information from all the 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, in contrast with our proposal, it has the weakness of not providing anonymity for users with respect to service providers.

Another similar approach for ticket based service access is described in [7]. According to our categorisation in this proposal, tickets are pre-paid, type t_3, and acquired following the outlet model. The importance of the customer care concept is not identified. Anonymity can be provided for all services for which it is deemed appropriate. Our proposal is more general because it allows for more ticket types and identifies the importance of the customer care role.

6 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 greater user satisfaction and new forms of business.

In order to make this feasible, we have identified two conditions that must 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 providing the users with tickets 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, 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. In *Proceedings of the 13th Annual Computer Security Applications Conference*, 1997.

[2] L. Buttyán and J-P. Hubaux. Accountable anonymous service usage in mobile communication systems. EPFL SSC Technical Report No. SSC/1999/016, 1999.

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

[4] G. Horn and B. Preneel. Authentication and payment in future mobile systems. In *Proceedings of ESORICS'98*, 1998.

[5] K. Martin, B. Preneel, C. Mitchell, H. Hitz, A. Poliakova, and P. Howard. Secure billing for mobile information services in UMTS. In *Proceedings of IS&N'98*, 1998.

[6] D. O'Mahony, M. Peirce, and H. Tewari. *Electronic Payment Systems*. Artech House, 1997.

[7] B. Patel and J. Crowcroft. Ticket based service access for the mobile user. In *Proceedings of Mobicom'97*, 1997.

[8] R. Rivest and A. Shamir. PayWord and MicroMint: Two simple micropayment schemes. *Cryptobytes*, 2(2):7–11, May 1996.

[9] U. Wilhelm, S. Staamann, and L. Buttyán. On the problem of trust in mobile agent systems. In *Proceedings of NDSS'98*, 1998.