Institut Eurécom
2229, Route des Crêtes
BP 193
06904 Sophia Antipolis
FRANCE

Research Report 94-012

# Untraceability in Mobile Networks

Refik Molva, Didier Samfat

October 24, 1994

Refik Molva, Didier Samfat
E-mail: {molva, samfat}@eurecom.fr
Tel: (+33) 93 00 26 12, (+33) 93 00 26 31
Fax: (+33) 93 00 26 27

# Contents

## Abstract

User mobility is a feature that raises many new security-related issues and concerns. One of them is the disclosure of the mobile user real identity during the authentication process, allowing an unauthorized third-party to track the mobile user's movements and current whereabouts. Therefore, accessing any information related to the mobile user's location data without his consent is a serious violation of his privacy. The basic solution to this problem is the use of *aliases* which insure non-traceability by hiding the user's real identity and also his relationship with domain authorities. However, this new issue is a conflicting requirement with respect to authentication, as non-traceability requires hiding the user's identity in contrast with authentication that requires the user's identity to be revealed in order to prove it. In fact, what is needed is a single mechanism reconciling both authentication and privacy of mobile user's identification. In this paper we present an efficient method for the computation of user's aliases which is applied to a new set of inter-domain authentication protocols that take into accounts five degrees of untraceability requirements. In doing so, we try to avoid the drawbacks of existing approaches such as CDPD and GSM. A pattent application has been submitted for the basic alias computation method.

# Untraceability in Mobile Networks

*Refik Molva, Didier Samfat*
*Institut Eurécom, Sophia-Antipolis, France*
*{molva, samfat}@eurecom.fr*

## 1 Introduction

Digital informations are becoming more and more important in everyday life. Pepole are often lead to provide identification information about themselves to organisations in order to obtain some services. Many examples can be found in existing systems, varying from a payement with a credit card to an access to the Internet. However, the common factor of such evironments is that during any of this transaction, the user have to provide an identification to the system. If no care is taken, a third-party may tap this identity and thus know who is involved in the specific transaction and where it is performed Even if in some contexts these details can be seen as a minor problem, ideally, unrestricted access to a person identification or location data is considered to be an unacceptable invasion of privacy until it is explicitly revealed by the person.

In mobile networks, a similar problem akin to mobility is the unauthorized tracking of users' migration. Independently of the topology of the network (wireless/cellular networks and wired networks supporting mobility), a typical situation arises when a mobile user (with or without a device) registered in a *home* domain pops up in a new foreign domain. In order to obtain services, the mobile user needs to prove his good standing to the visited domain. A well-known solution is the authentication which requires the home authority to confirm the solvency of the user in the visited domain. Usually, during this process the user has to provide a non-ambiguous identity to his home domain and has to prove it. As this identity can be tapped by an eavesdropper (on the air interface in a cellular environment or through the signalling protocols exchanged on the wired network registered), it allows an unauthorized third party to know when the user is accessing the network and where he is located. However, hiding only the user's real identity is not sufficient to fullfil the untraceability requirement as its disclosure may be obtained by analysis of any information related to the user's relationship with domain authorities. Therefore, if perfect privacy is required, no entity other the user himself should know the real identity or the current location of the mobile unit.

This paper is organized as follows. We begin in section 2 by presenting the issues of untraceability on behalf of the user interface. Section 3 summarizes the drawbacks of existing solutions. In Section 4 we make a classification of different level of identity privacy which potential solutions should take into account. Section 6 present different approaches for untraceability of mobile user. Some evaluations of the different proposed solutions are made in section 7. Section 8 concludes with the summary of the paper.

## 2 Untraceability and Its Implication

In certain situations, mobile users are unwilling to reveal information related to their location or movements; therefore, untraceability becomes an important requirement as it will provide users additional privacy. The basic technique requires the use of aliases instead of the real user identity. However, using aliases has different issues depending on the mobile environment and the user interface involved.

### 2.1 Aliases and Elementary End-User Interface

In the case of a wireline network supporting mobility, a user may have only a password or PIN for the purpose of authentication [8]. Therefore, users have to provide their credentials in order to access the service and are forced to rely on the available public access equipment (i.e workstation or public terminal). We can reduce this exposure by using traveling aliases in order to avoid the visiting domain to know the real identity of the user. Therefore, even if the public access equipment knows the password of the user, it does not know *whose* credential it is.

However, this alias should be a character string as human friendly as the usual user name. The only condition on the generation of this alias is that it should not be related to the user name at the home domain. The advantage resides in the choice of such an alias which is not subject at all to the same considerations as the generation of a secret password. In the case of passwords, the security requirement is to make the guessing of the value hard and the goal is to choose a password as weird as possible so that a straight forward search through the list of known words would not easily guess its value. As aliases are sent in clear text, there is no need to choose weird words; common words of the dictionary are sufficient.

Nevertheless, a similar attack can be done in this kind of situation. Having the password of the user, a malicious workstation can scan a list of pre-established aliases in order to know whose password belong to. Little can be done in this situation unless the user changes his alias regularly. In that case, the user will need a list of traveling aliases easy to remember.

### 2.2 Aliases and Advanced End-User Interface

In contrast to the elementary end-user interface, mobile user in possession of a trusted device (smartcard, portable phone) can benefit from reduced exposure by having better random aliases which can be changed more frequently and in a transparent way. In fact, the end-user terminal can share additional specific information with his home authority in order to generate strong random aliases. Potential solutions should take into account different levels of privacy as described below in section 4.

### 2.3 Aliases vs. Accounting and Billing

Alias techniques provide users with anonymity while keeping the foreign domain authority "in the dark". Hence, non-traceability can be undesirable when accounting and billing are involved. However, the foreign authority can still keep a trace of the user by recording the proof of use and thus ask the home authority to be "refunded". Therefore, alias solutions are not in contradiction with accountability/billing providing to the extent that they allow the home authority to recover the real user's identity in order to invoice the right user.

# 3 Review of Existing Approaches

In this section, we review existing approaches for untraceability in different environments varying from banking systems to mobile network.

## 3.1 Untraceable Electronic Cash

Providing anonymity to users is not a new feature. We present here some mechanisms which have been developed for banking environment [9, 10].

The first mechanism provide the untraceability of the payment transaction. The basic idea is to avoid the disclosure of information related to the different purchases of the customer. At an initializing step the customer change his money into an electronic bond certified by the bank (encrypted under the bank's private key). When the customer has to make a payment, he gives this bond to the shop which verifies its content using the bank's public-key. Next, the shop is able to change this bond into cash money at the bank. As all bonds have the same format it is impossible for the bank to make any correspondence between withdrawal of users and deposits of shops.

The main concern with this approach, is that withdrawal from a bank or making a payment requires the user to be authenticated by both the bank and the shop (e.g PIN and smartcard). Therefore, even if the payment is untraceable, the identity of the customer is revealed to the bank as well as to the shop. A solution based on this approach may be envisioned for the purpose of allowing the user to access a service in the mobile network. However, in addition to this mechanism, the authentication process should not reveal the identity of the user. Moreover, if perfect anonymity is required, the relationship of the user with his home authority (and also with foreign authorities) should be protected.

The second mechanism allows the computation of untraceable credentials. When the user need to share a pseudonym with an organization he must compute a list of potential pseudonyms. Then, he communicates this list to a "credential clearinghouse" which chooses a pseudonym and signs it with its private-key. Upon receiving the certificate, the user sends it to the organization which verifies the chosen pseudonym by using the clearinghouse public-key.

In this case, even if the real identity of the user is not known to organizations, all pseudonyms are revealed to the clearinghouse. Moreover, it requires the use of at most one long static pseudonym per organization; an eavesdropper tapping the network can make a correlation between this pseudonym and the user's real identity by traffic analysis after a certain time. Hence, changing frequently pseudonyms becomes an important requirement which is not supported by this approach. Therefore, in a high dynamic mobile network environment such as wireless networks, generating a list of pseudonym is not efficient in term of both bandwidth consumption and the overhead incurred to the user.

In fact what is needed, is a single efficient mechanism allowing a user to access the service of the mobile network while keeping his identity secret as well as the access control mechanism from unauthorized (and authorized) parties.

## 3.2 GSM

The Global System for Mobile GSM is the first digital cellular network to provide anonymity to his subscribers. In GSM, non-traceability is provided by using Temporary Mobile Subscriber Identifiers (TMSI). But the main concern with GSM is when a user first switches on his portable phone his International Mobile Subscriber Identifier (IMSI) is transmitted in clear through the radio path (the TMSI is only allocated after this step). In that case, if the user is continuously tracked, his real identity is revealed and therefore it is possible for an eavesdropper to correlate this IMSI with the following assigned TMSIs.

An other point of contention with GSM is that the fixed network is assumed to be secure and therefore all visited domains know the real identity of the mobile unit. Because location data are conducted in clear through the fixed network they do not provide identity privacy to the subscriber.

### 3.3 CDPD

In contrast to GSM, *CDPD* [7] has a more secure approach. Before the authentication procedure takes place, the mobile unit engages a Diffie-Hellman key exchange protocol in order to share secret session key with the visited authority. Next, the mobile unit enciphers its identity with this new key and transmits it to the foreign authority which deciphers the encrypted identity with the same shared secret key.

This first drawback of this approach , is that it allows the visited authority to know the real identity of the mobile unit. The second drawback remains the nature of the Diffie-Hellman protocol which allows an intruder to masquerade as the visiting authority and to discover the mobile unit real identity.

We have seen different mechanism providing anonymity to users. Even if the above presented approaches are reasonable in their context the same cannot be guaranteed if perfect privacy is required. Therefore, providing total anonymity to mobile users requires to hide the user real identity from both unauthorised parties (eavesdroppers) and authorised parties (remote administrative authorities). In addition to these requirements, potential solutions should take into account different degrees of privacy as described in the next section.

## 4 Classification of Untraceability Requirements

Hiding the user's identity is not always sufficient to fulfill the non-traceability requirement. An additional requirement is to hide various relationships between the user and the administrative authorities. Therefore, we have defined five classes of user's identity privacy depending on the expected level of security.

- *C1: Hiding User Identity from Eavesdroppers.* Most of the existing solutions address this requirement. In GSM, the use of TMSIs is used by way of aliases. However, the basic requirement is that derivation of successive alias should not lead to the disclosure of the real user's identity. In that sense, we can envision different ways in assigning aliases to mobile users during their migration.

  When the user appears for the very first time in a new foreign domain, he needs to establish a temporary residency with the foreign administrative authority. At this step an long-term alias can be assigned to the user for his stay. The main problem with this approach is that all activity performed in the remote domain can be linked with a single alias. After a while, the relationship between this alias and the user's home domain can be discovered by traffic analysis.

For this purpose, in a more secure way, each time the user accesses a service in the visiting domain, a different alias should be assigned avoiding the disclosure of his relationship with the foreign authority.

- *C2: Hiding User Identity from Foreign Authorities.* There is no need for a foreign authority to know the real identity of the user. What it needs is only a proof of the solvecy of the entity accessing the service and enough information to bill the user's home authority.

- *C3: Hiding Relationship Between the User and Authorities.* In a higher level of privacy, it is important to protect the existing relationship between the mobile user and his home authority from a third-party. The real identity of the user may be discovered by traffic analysis between the foreign and the home authority. In other words, each time the user accesses the network, if his home authority identity is not protected, a correlation can be made with the user's real identity.

  For instance, knowledge of the relationship between the aliases $x, y, z$ and their home domain $D$ might help an intruder to come up with the conclusion that these aliases replace identities of users $A, B, C$ out of domain $D$, if $A, B, C$ are the only users of domain $D$ that can travel outside their home domain.

- *C4: Hiding the Identity of the Home Authority from Foreign Authorities.* When the mobile user needs to be authenticate in a foreign domain, the foreign authority needs to contact the user's home authority in order to have a confirmation of the good standing of the user. Therefore, even if the real identity of the user is hidden, his relationship with his home is known by the foreign authority.

- *C5: Hiding User Behaviour from Home Authority.* In some cases it might be important for a mobile user to hide his migration from his home authority. This requirement is specially important if perfect secrecy of user behaviour should be guaranteed by the system, that is, if no one other than the user should know about the user's location. This principle of course would contrast the intent of a "big brother" towards global observation of users' behaviour.

## 5 Reconciling Authentication and Untraceability

Untraceability is a conflicting requirement with respect to authentication, as non-traceability requires hiding the user's identity in contrast with authentication that requires the user's identity to be revealed in order to prove it. In this section we present a solution for the computation of aliases which can be used to protect the identies of the different parties involved in the authentication process.

### 5.1 Initial Assumptions

We begin by stating that a user has one *home* which is the administrative domain where he is registered on a long-term basis. Moreover,when accessing the network in the *home* domain, the mobile user is authenticated with a traditional server-based authentication mechanism such as Kerberos [2] or KryptoKnight [3]. Users of every network domain are registered with that domain's Authentication Server (AS). The AS of a domain can be replicated or

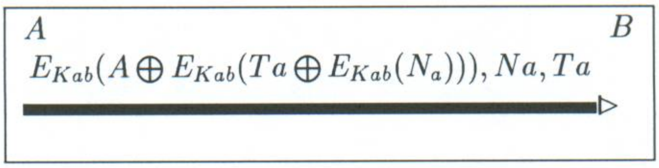

Figure 1: One-Way Authentication Protocol

partitioned within the domain but the set of all partitioned and duplicated ASs represent a single domain-level authority.

We assume that the user has a personal device which can store information, because little can be done for non-traceability of mobile users having only their user-name and password (or PIN) for authentication as described in section 2.

Moreover, the user need a universal identification (for example home user identification) to which only the home domain can linked the different aliases. This is particularly important for a central authority specially when accounting and billing are involved.

## 5.2 Design Criteria

In order to insure a good anonymity to the mobile user during his migration, solutions must take into account the following design criteria:

- *One-time-use alias.* Long-term use of a single static alias is not a good solution, as it may be cracked or correlated to the user's real identity. Consequently, it is desirable to use one different alias at each security process.
- *No direct relationship between aliases.* This is quite an obvious but important requirement, as we want to hide effectively the user identification.
- *Domain separation.* Assuming the conspiracy of all visited domains (except the home domain) the real identity of the user should not be discovered.

## 5.3 Protocol Building Blocks

We base our design on the one-way authentication protocol (see figure 1 borrowed from *KryptoKnight* an authentication and key distribution service developed at IBM Research [3].

The expression in figure 1 is computed as a result of applying a strong encryption function $E$, e.g., DES [6], with $Kab$ as the encryption key, over three inputs: one nonce ($Na$), a timestamp ($Ta$) and the name of the message originator. In the rest of the paper $AUTH_{ab}$ will denote the one-way authentication of an initiator $A$ to a responder $B$.

## 5.4 Alias Computation

KryptoKnight does not provide identity privacy as the initiator $A$ sends his identity in clear to the responder $B$. Therefore, if we want to protect an identity $A$ from an unauthorized party, we need to compute an alias which the responder $B$ can understand. The basic idea of this solution rely on the fact that using shared-secret keys always need an identity to be provided in contrast to public-key where the identity is implicit. An alias for the principal $A$ can be computed as follow:

$$P_b(N_a, N_a \oplus A)$$

$P_b()$ denotes the result of the encryption with the responder's public-key over two inputs: one nonce and the identity of the initiator. Upon receiving the alias, $B$ deciphers $N_a$ then $N_a \oplus A$ with his secret-key $S_b$ then obtain $A$ by doing $N_a \oplus N_a \oplus A$.

# 6 Untraceable Authentication Protocols

Many cryptographic solutions are possible for the purpose of insuring anonymity to mobile users. The main distinguishing factor is the level of identity privacy needed. Therefore we develop three authentication protocols taking into account the five classes of privacy as described in section 4. In doing so, we avoid the drawbacks of GSM and CDPD and provide an appropriate solution for untraceability of mobile users in contrast to the "Electronic-Cash" approach. 4.

## 6.1 Basic Protocol

The basic untraceable authentication protocol is depicted in figure 2. The main idea is to generate and use at each security transaction a random alias. The following notation is used in this protocol:

- $Uid$ – Universal identification of the end-user $U$ in his home domain
- $Uid_x$ – Identification of the user in domain $X$
- $AS_h$ – Authentication Server of the home domain
- $AS_r$ – Authentication Server of the remote domain
- $K_u$ – Key shared between $U$ and $AS_h$
- $K_{rh}$ – Long-term key shared between $AS_r$ and $AS_h$
- $K_{ur}$ – Key shared by the user with $AS_h$ and given by $AS_h$
- $P_h$, $S_h$ – Public-key, Secret-key pair of $AS_h$
- $P_r$, $S_r$ – Public-key, Secret-key pair of $AS_r$
- $N_u$ – Nonce issued by the access device on the user's behalf
- $N_r$ – Nonce issued by $AS_r$
- $P_x(A)$ – Encryption of message $A$ with the public-key $P_x$
- $AUTH_X$ – Authentication message computed by $X$. $AUTH_X$ is a challenge message composed of a clear-text part and an authentication token.
- $TICK_{K_x}(K_s)$ – A ticket computed with the key $K_x$ and containing a session key $K_s$
- $\oplus$ – exclusive-or operation (xor).

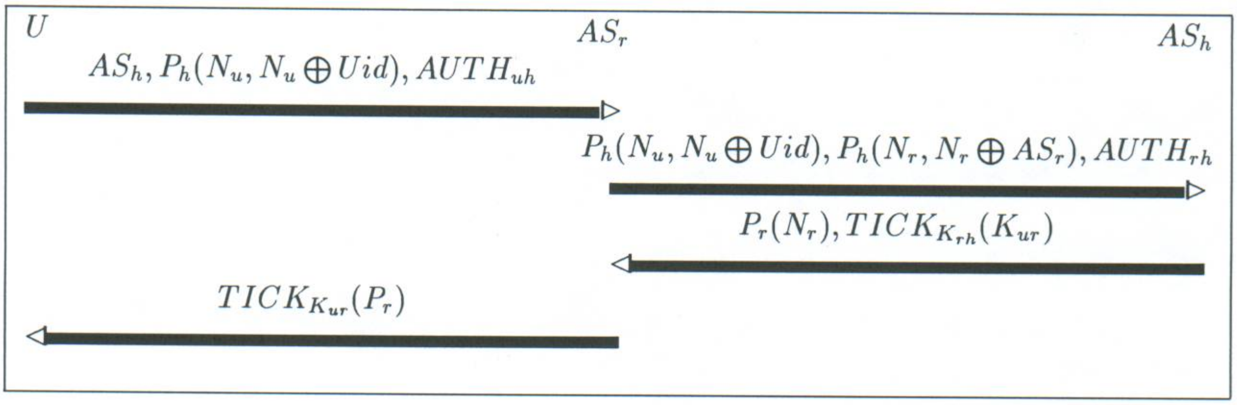
$U$
$AS_r$
$AS_h$
$AS_h, P_h(N_u, N_u \oplus Uid), AUTH_{uh}$
$P_h(N_u, N_u \oplus Uid), P_h(N_r, N_r \oplus AS_r), AUTH_{rh}$
$P_r(N_r), TICK_{K_{rh}}(K_{ur})$
$TICK_{K_{ur}}(P_r)$

Figure 2: Basic Untraceable Authentication Protocol

This protocol provide class C1 and C2 of identity privacy as neither the user nor the $AS_r$ identity are disclosed during the authentication process. The basic requirement is that the user's device has to store on a long-term basis his home domain public key $P_h$. We now turn on the details of the protocol:

1. The user begins by generating a nonce $N_u$ and stores it in his device. Next, he computes both his alias $P_h(N_u, N_u \oplus Uid)$), and his one-way authentication message using his home key $K_u$ . Then, he sends these messages to the local $AS_r$ along with $AS_h$ identity. Note that at this step the relationship between the user and his $AS_h$ is revealed, but we can add another level of privacy as described in the section section 6.2.

2. Upon receipt of the initial message, $AS_r$ issues a nonce $N_r$, saves $P_r(N_r)$ in its database; the reasons for this encryption will be explained below. Next, it generates its own alias $P_h(N_r, N_r \oplus AS_r)$ , then computes his authentication message containing $AUTH_{uh}$ using a token chaining technique. Further details on this kind of authentication technique are described in [4].

3. When $AS_h$ receives the message in flow 2, it proceeds as follow:

   (a) It deciphers $N_u$ and the user's alias with $S_h$. Then $Uid$ is obtained by applying once again the xor operation.

   (b) $AS_h$ recovers $AS_r$ identity in the same way

   (c) Having $Uid$ and $AS_r$, $AS_h$ is able to look for the corresponding shared secret keys in his database and recomputes $AUTH_{rh}$

   (d) A match in this last step authenticates both the user and $AS_r$ without revealing neither $Uid$ nor $AS_r$ identification to a third-party.

   (e) As $AS_h$ needs to send a ticket containing the location dependent key $K_{ur}$ to $AS_r$, it just has to return $N_r$ ciphered with with $AS_r$'s public key along with the ticket.

   In fact, $P_r(N_r)$ is saved in $AS_r$'s database in order to avoid the home AS to compute and send his alias in flow 3. This value can be seen as a secret transaction number which identify the authentication process involving both the user and $AS_h$. In other words, this transaction number allows $AS_r$ to know who is sending the ticket and to whom belongs $K_{ur}$ while insuring anonymity to the home AS as well as to the user.

The reason for $AS_r$ to record the encrypted form of $N_r$ is to avoid its deciphering upon receiving the response from $AS_h$. This has the advantage to reduce the computation operation with the $S_r$ as an immediate comparison with the value send by $AS_h$ in flow 3 can be done.

4. This flow is purely optional as it allows $AS_r$ to give the user his public key $P_r$ [1]. This key will be used by the user during future single-sign-on with $AS_r$ for the computation of new aliases.

Once the user has established a residency in the remote domain with the identification $Uid_r$, e.g. $P_h(N_u, N_u \oplus Uid)$, he may vary this identity on the next single-sign-on using the same alias computation technique as in section 5.3. The user issues a new nonce $N_1$ and provides the following messages along with his authentication message:

$$P_r(N_1, N_1 \oplus Uid_r)$$

Upon receiving this message, $AS_r$ is able to recover $Uid_r$. Therefore, this technique allows the user to vary his identity in the remote domain at every authentication process.

## 6.2 Enhancing the Level of Anonymity

The basic protocol lacks of providing the secrecy of the relationship between the user and his home AS because $AS_h$ identity is revealed in flow 1. In order to have an additional degree of privacy as described in section 4, the user need to compute an alias for $AS_h$. As the mobile user does not have $AS_r$'s public-key, before the authentication protocol starts the user may ask $AS_r$ [2] for a public-key certificate containing $P_r$. Figure 3 depicted the revised protocol:

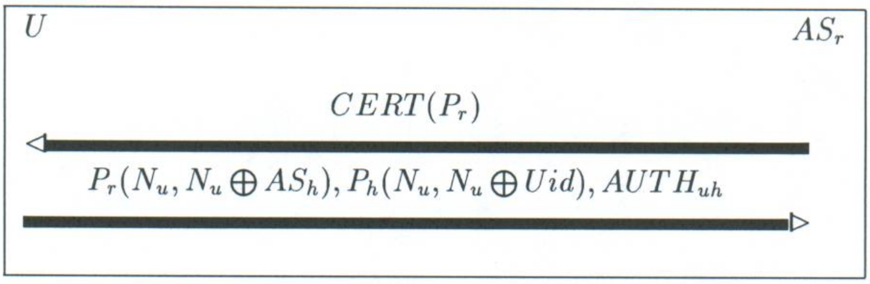
$U$
$AS_r$
$CERT(P_r)$
$P_r(N_u, N_u \oplus AS_h), P_h(N_u, N_u \oplus Uid), AUTH_{uh}$

Figure 3: Protocol Hiding Home Domain Authority to Unauthorized Third-Party

If an anonymity of class C3 is required then the use of a trusted Certification Authority (CA) is mandatory. Such a CA can be a specialized AS which main purpose is to deliver public-key certificates to all other ASs. Therefore, an additional requirement is that the CA's public key should be stored in the mobile equipment at subscription time.

When accessing the network, the user receives the certificate containing $AS_r$ public key ($CERT(P_r)$) from $AS_r$. A CA's certificate can be computed as follow:

$$CERT(P_r) = S_{ca}(Index, DateOfIssue, Lifetime, P_r)$$

Upon receiving $CERT(P_r)$, the user decipher the certificate using the CA'S public-key $P_{ca}$ and retrieve $AS_r$'s public-key $P_r$. Next, he computes an $AS_h$'s alias using $P_r$ allowing

[1] The certificate containing $P_r$ can be given to the user by another mean

[2] if available may retrieve the certificate from a database

only $AS_r$ to know the real identity of the home AS. It is expected that flows 3 and flow 4 of the basic protocol in figure 2 (involving the home domain) are performed in order to accomplish the protocol cycle.

## 6.3 A Full Untraceable Authentication Protocol

Until now, we have presented two protocols forcing mobile users to contact their home domain for the purpose of authentication. Figure 4 depicts an authentication protocol avoiding the mobile user to "call home". In this protocol, the user has already been authenticated in domain $A$ and shares a secret key $K_{ua}$ with $AS_a$ [3]. When the user arrives in a new domain $B$ he proves his identity by requiring $AS_a$ to confirm his solvecy to $AS_b$. The following additional notation is used:

- $\overline{X}$ – Alias computed for principal X using the public-key technique as defined in section 5.3.
- $\overline{Uid_a}$ – Alias used by the user in domain A
- $K_{ua}$ – Key shared by the user with the AS of domain $A$ ($AS_a$)
- $K_{ub}$ – Key shared by the user with the AS of domain $B$ ($AS_b$)
- $N_b$ – Nonce issued by $AS_b$
- $P_b(N_b)$ – Secret transaction number as described in section 6.1

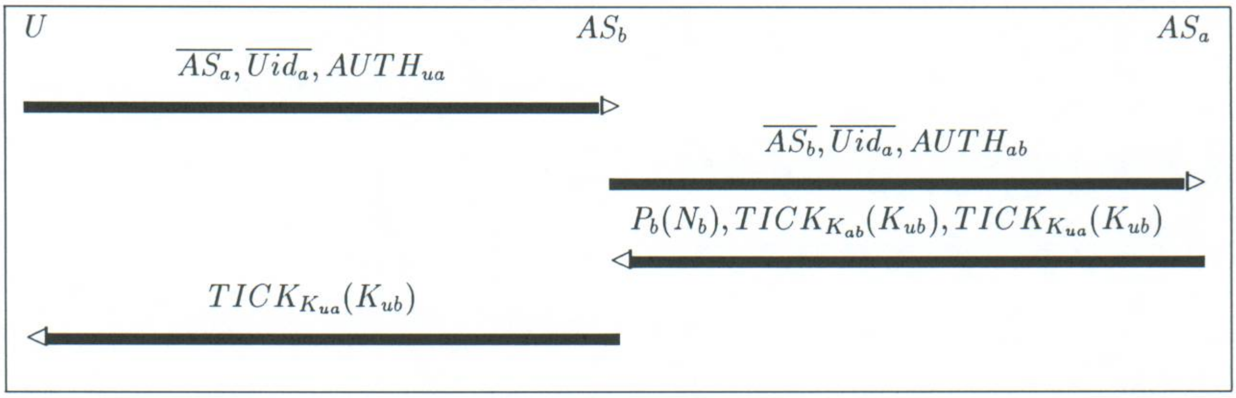
$U$
$AS_b$
$AS_a$
$\overline{AS_a}, \overline{Uid_a}, AUTH_{ua}$
$\overline{AS_b}, \overline{Uid_a}, AUTH_{ab}$
$P_b(N_b), TICK_{K_{ab}}(K_{ub}), TICK_{K_{ua}}(K_{ub})$
$TICK_{K_{ua}}(K_{ub})$

Figure 4: Protocol Involving Adjacent Remote AS

The basic idea of this protocol, is that the user doesn't have to contact his home AS in order to be authenticate. In fact, the user just needs to provide the alias of a previous visited-domain's AS which can guarantee his solvency. This protocol provides class C4 and C5 [4] of identity privacy as the user's migration is hidden to his home domain and $AS_h$ real identity is not revealed to the visited domain $B$.

[3] This step may have involved the home domain using the previous protocol

[4] In addition to class C1, C2 and C3 of identity privacy

# 7 Protocol Evaluation

In this section we make a discussion on the proposed solution in contrast to other possible designs. We make also an evaluation along the lines of the previous stated design.

## 7.1 Other Designs

Other solutions based on a common pre-computed list of alias kept on behalf the user equipment and his home AS are possible. However, such techniques need to share a common state between the mobile equipment and the home domain. The issued aliases can only hide the identity of the user in the foreign domain but not his relationship with the home authority.

Another problem arises when all aliases of a list have been used: in this case, the home domain has to generate on-the-fly a new alias list and has to communicate it to the mobile. This requires either a secure channel between the user and his home or an additional secure protocol to transfer the new aliases. These features are not always available in every mobile environment.

A final remark on such solutions is that the mobile equipment and the home AS has to be continuously synchronized in order to choose the same alias in the same time. Otherwise, an additional mechanism is thus needed for the recovering of the common state when a gap occurred. Our protocol avoids all these constraints.

## 7.2 Computational Complexity of the Protocols

The expensive computation part of a public-key cryptosystem remain typically to the private key operations. However, public-key algorithm such as RSA [11] chooses the keys in order to minimize both the signature verification process and the public key encryption process. In addition to this, new public-key algorithms with lower complexity have been developed for wireless network and are efficient in real time [12]. Therefore, in order to evaluate the efficiency of the protocol, we need to count the total number of the private-key operations.

In the basic solution, $AS_h$ needs to decipher both the user's alias and $AS_r$'s alias. In the enhanced version of the protocol, one additional encryption operation is needed as $AS_r$ needs to perform another decryption operation on $AS_h$'s alias.

Thus, the total computationally expensive operations come to two in the basic solution and to three in the second solution. In other protocol based on a combination of the Diffie-Hellman key agreement protocol using digital signatures for authenticity [13], a total of six computationally expensive operations are needed but such scheme does not provide anonymity to users.

## 7.3 Evaluation of the Alias Solution

The alias computation solution meet the design goals as described below:

- **One-time-use alias.** The first time the user accesses the network, he computes an alias. On a next access he is endowed with a new alias by using the changing alias procedure.

- **No direct relationship between aliases.** Each alias is computed by issuing a random number. For the first alias $P_h(N_u, N_u \bigoplus Uid)$ it is impossible to make any correlation with future aliases as they are only random numbers.

- **Domain separation.** Even conspiracy of every ASs, it is impossible to find any relationship between aliases (random numbers) of different domains and to derive the real user's identity from them. Only the home domain is able to recover the real user's identity from the first aliase transmitted by the user.

# 8 Conclusion

In conclusion, this paper discussed of traceability of mobile users and its implications. Existing solution for the unauthorised tracking of user's migration such as GSM and CDPD presented some weakness in providing users good anonymity. We have presented an efficient method for the computation of user's aliases. The advantage of this method is that it can be used to hide the identity of all entities involved in the authentication process. Therefore, we have provided a new set of untraceable authentication protocol suitable according to the different degree of privacy desired.

# References

[1] M. Rahnema, *Overview of the GSM System and Protocol Architecture*, IEEE Communications Magazine, April 1993.

[2] J. Steiner, C. Neuman, J. Schiller, *Kerberos: An Authentication Service for Open Network Systems*, Proceedings of USENIX Winter Conference, February 1988.

[3] R. Molva, G. Tsudik, E. Van Herreweghen, S. Zatti, KryptoKnight *Authentication and Key Distribution Systems*, Proceedings of ESORICS'92, November 1992.

[4] R. Molva, D. Samfat, G. Tsudik, *Authentication of Mobile Users*, IEEE Network Magazine, Special Issue on Mobile Communications, March/April 1994.

[5] W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, November 1976.

[6] National Bureau of Standards, *Federal Information Processing Standards*, National Bureau of Standards, Publication 46, 1977.

[7] *Cellular Digital Packet Data (CDPD) System Specification*, Release 1.0, July 19, 1993.

[8] European Telecommunications Standards Institute, *Universal Personal Telecommunications*, ETSI NA7 WP1, November 1992.

[9] D. Chaum, A. Fiat and M. Naor, *Untraceable Electronic Cash*, Proceedings of Crypto'88, August 1988.

[10] D. Chaum, *Security Without Identification: Transactions Systems to Make Big Brother Obsolete*, CACM Vol. 28, No. 10, October 1985.

[11] RSA Data Security Inc., *The RC4 Encryption Algorithm*, Document No. 003-013005-100-000-000, March 12, 1992.

[12] M J.Beller, L F. Chang, Y. Yacobi *Security for Personal Communications Services: Public-Key vs. Private Key Approaches* Proceedings of 2nd International Symposium on Personal, Indoor and Mobile Radio Communications, October 1992.

[13] W. Diffie, P.C.V. Oorschot, M.J. Wiener *Authentication and Authenticated Key Exchanges in Designs, Codes and Cryptography* Kluwer Academic Publishers, 1992.