7

Anonymous Mobility Management for Third Generation Mobile Networks

S. Hoff, K. Jakobs, D. Kesdogan
Aachen University of Technology – Department of Computer Science – Informatik 4 (Communication Systems)
D-52056 Aachen, Germany,
Tel.: +49 241 80 21417, Fax.: +49 241 8888 220,
E-mail: {hoff, jakobs, kesdogan}@i4.informatik.rwth-aachen.de

Abstract

With the increasing use of mobile and nomadic communication devices requirements for security and privacy are rising as well. Following brief surveys of existing approaches to mobility management, general security considerations for UMTS and confidential storing of location information we introduce the ideas and concepts behind the new 'anonymous subscriber' method for UMTS, largely based on extended MIX networks. Finally, an application of this method conveniently employing the X.500 directory service infrastructure is described in some detail.

Keywords

Mobile networks, mobility management, security, privacy, directory service, X.500

1 INTRODUCTION

The degree of mobile and nomadic computing is expected to increase dramatically in the near future. As the users' demands increase with the services offered by mobile communication systems, the main expectation on such systems will be to provide access to any service anywhere anytime. UMTS - the Universal Mobile Telecommunications System - will be the future mobile communication network in Europe. It is supposed to provide a platform for existing systems of the second generation, based on standards like GSM, DCS1800. Up to now work on security aspects of UMTS focused on a comparison of different procedures for authentication purposes. Our goal is to improve privacy and trustworthiness of the system. That

P. Horster (ed.), *Communications and Multimedia Security II*

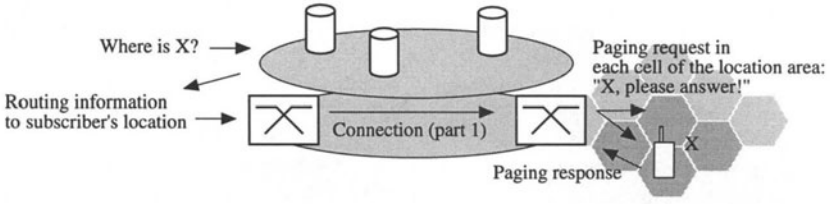
Where is X?
Routing information to subscriber's location
Connection (part 1)
Paging request in each cell of the location area: "X, please answer!"
X
Paging response

Figure 1 General principle of mobile terminated connection establishment.

is, we are designing mechanisms to prevent third parties from generating moving tracks of users. This implies that the protection should be shifted into the domain of the user, where the administration of the location information of his/her mobile station should be handled as far as possible. The user should be able to act anonymously whenever possible. The location management strategy presented in this paper provides the roaming user with anonymity, thus fulfilling the demand for privacy.

Section 2 reflects on location management in the second and third generation of mobile networks. Security considerations for UMTS are summarized in section 3. Section 4 provides an overview of earlier attempts to solve the problem of location management. New location management strategies for UMTS considering privacy are introduced in section 5. Finally, section 6 discusses the applicability of the new method in UMTS when using X.500 to implement the UMTS distributed database*.

2 MOBILITY MANAGEMENT IN MOBILE NETWORKS

Characteristic tasks of a communication system in a mobile environment include radio resource management, mobility management, service management and security management, resulting in architectures different from networks interconnecting fixed stations only (Spaniol et al., 1995). In contrast to conventional tele- and data communication systems, a mobile network has to keep track of a subscriber's current position to enable routing of incoming calls and continuous communication. To achieve this, the concept of location areas has been introduced. A *location area* is the smallest unit for which the mobile network maintains the current location of a subscriber, i.e., a location area is a group of cells with an associated database storing the identifiers of mobile stations currently registered. As subscribers will enter and leave a location area dynamically, the corresponding entries in the database will have to be updated accordingly. Upon a mobile terminated incoming call, the network transmits *paging messages* only to those cells of the location area where the mobile station is currently registered. When the called mobile station answers this paging message, the network knows the cell where the station is located and a communication link can be established (Fig. 1). Existing schemes for mobility management mainly differ in the process how to decide on a location update (Bar-Noy et al., 1995), and in the techniques used to maintain the location information in the fixed network, see (Wang, 1993), (Madhow et al., 1994), (RACE D733, 1995).

* X.500 is a major candidate for the internal structure of the UMTS distributed database (RACE D733, 1995).

The digital second generation systems based on the GSM standard have been replacing their first generation analog predecessors since 1992. The mobility management in GSM is based on a *centralized approach* (Rahnema, 1993). The Home Location Register (HLR), a central database of a PLMN*, maintains a reference to an Mobile Switching Center (MSC) with an associated Visitor Location Register (VLR), where the mobile station is currently registered and the corresponding location information (i.e., the identifier of the location area) is stored. Upon location update, the entries in the affected VLRs and in the HLR are updated (via Signalling System No. 7). For each incoming call the HLR is interrogated first. If it accepts the service request, the routing information addressing the visited MSC/VLR is returned.

Third generation mobile systems** will have to cope with various telecommunication and data communication services as well as the migration of mobile and fixed networks into one global worldwide universal communication system. UMTS enables Universal Personal Communication, i.e. communication anywhere, anytime, mobile or fixed, with a single "telephone" number (Rapeli, 1995), addressing the subscriber rather than the device. Services and applications currently investigated, e.g. mobile multimedia (Armbrüster, 1995), will also have an impact on the layout of the cellular network: It cannot be expected that multimedia services are offered in the whole network in the medium term, maybe only in in-house subnetworks. Hence, service quality and service offer will change dynamically with handovers and location updates. Service handling and mobility management will be based on Intelligent Network concepts, see for example (Jabbari, 1992), (RACE D733, 1995). The expected variety of services, the very large number of subscribers and the areas to be covered by a third generation network make a centralized mobility management almost impossible. In addition, the specific communication profiles of subscribers as well as the applications and services they use (e.g. speech, fax, X.400, etc.) require new management schemes, see (Spaniol et al., 1995), (Fasbender et al., 1995) and (Wang, 1993).

3 SECURITY CONSIDERATIONS FOR UMTS

The special security problem in UMTS stems from the objective of global reachability and easy service access for the users, i.e. the user should be able to go everywhere and use the subscribed services via the air interface in an easy way. Characteristic vulnerable points caused by the mobile and global nature of UMTS include:

- air interface: easy tapping of the medium,
- access network: changes with the location of the users and should provide an easy access point to the user and prevent unauthorized use of resources,
- the distributed structure of UMTS: different network operators and service providers work together and must guarantee the security of the exchanged information,
- databases: stores private data, i.e. localization information in order to ensure global reachability, secret key information to ensure access rights and other information to facilitate a user specific service.

* PLMN = Public Land Mobile Network

**In Europe a Third Generation Mobile System referred to as *Universal Mobile Telecommunications System* (UMTS) is specified by ETSI

The risks resulting from these vulnerable points of UMTS include illegal information collection, unrecognized change of information and disturbance of the functionality by unauthorized third parties. To this end security requirements are availability, integrity and confidentiality:

- Availability: the communication network enables communication between all parties who wish to communicate (and who are allowed to do so).
- Integrity: data are received correctly and completely, integrity of the sender is guaranteed, and a trustworthy receipt notification is provided.
- Confidentiality: data is only available to authorized persons.

The RACE specifications for UMTS foresee protection measures to support those security requirements, but do not provide any mechanisms to actually solve the problem, see (RACE 1043, 1991) and (RACE D731, 1994). The operational UMTS objectives in the security area specified in (RACE D731, 1994) include:

1. protecting end-to-end user information and system information flows using encryption,
2. protecting the privacy of the user and the system's knowledge of the location of the user,
3. mutual authentication of the user and the service provider,
4. terminal equipment identification.

Until now specification efforts were directed towards the comparison of different cryptographic techniques and their key management issues, to be employed in identification and authentication procedures.

Our objective is to protect the privacy of the user by protecting the system's knowledge of the location from access by third parties. Usually the network operator has unlimited access to the managed databases and is able to trace the user of a mobile station and construct moving tracks without the user's knowledge (Federrath et al., 1995). In UMTS this risk is even higher as it will be a conglomeration of network providers and service providers. Hence, to control who has access to which data will not be a trivial task. In any case, however, the unlimited access of the network operators violates the subscriber's privacy. This, in turn, leads to the violation of the data security requirement "confidentiality". The following sections present methods increasing the subscriber's privacy by an anonymous management of the location information.

4 CONFIDENTIAL STORING OF LOCATION INFORMATION

One approach to store location information in line with the above security requirement is to keep them within a trustworthy environment. Pfitzmann (1993) proposes to store confidential information in a personal digital assistant or "personal communication bodyguard". A HTD (Home Trusted Device) is the most common realization of such a trusted and private environment. In the following we will explain the role it could play in location procedures in a GSM like system.

The HTD has to play the role of both HLR and VLR. Thus, the location registration and the location cancelation take place at the HTD rather than the VLR and the HLR. To establish a connection to a mobile user, the network requests the current location of the user from his/her HTD. The functionality of the HTD is not restricted to the role of a location register. It should perform reachability management procedures to detect abusive requests from a third party

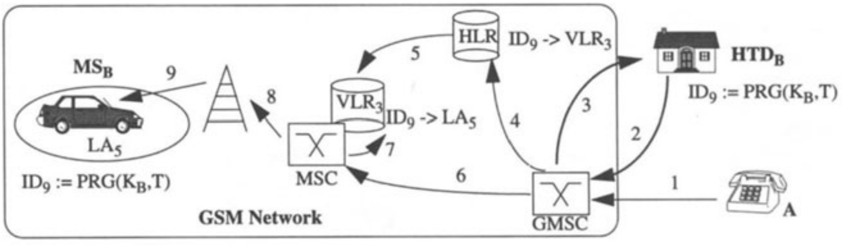

Figure 2 Call setup with centralized AS-Method.

trying to trace the mobile subscriber, using for example the "neither or both" information exchange. Neither or both means that a request will not be honored if the requester does not unveil his/her identity. An HTD acting as a Location Register in conjunction with a reachability management machine is one way to enable each user to control the security of his/her own confidential information.

Another approach allows both, to store the subscribers' exact location information in central databases and to guarantee the subscribers' privacy, see (Kesdogan et al., 1996), (Kesdogan et al., 1995). This is called the "Anonymous-Subscriber" (AS) strategy with a Home Trusted Device (HTD). The basic idea of this strategy is to allow entries in HLR and VLR holding exact location information only if the subscriber remains anonymous. The network is time synchronized, and at time t_i all users in every location area transmit an implicit address to the network, see (Farber et al., 1975), (Karger, 1977). This implicit address is quite long (e.g. 50 to 100 Bits) and will be considered as a pseudonym by the network administrator. The source of the implicit address is a pseudo random generator (PRG) with the secret key k_B. This implicit address is built into the user's MS and the user's trusted HTD.

In Fig. 2 user A wants to communicate with mobile subscriber B. First, the network needs the current pseudonym ID_B of B. It requests the trusted private environment HPC of B for ID_B. To protect against surveillance of B's location the requests have to be audited by the HTD. In the HLR the entry <ID_B, VLR> is used to route the call to the responsible current LA of the pseudonym ID_B, and generates the paging message.

This approach requires an HTD and is not directly applicable to the mobility management in UMTS. The requirements on UMTS are to serve mobile users globally, and if the mobile user has been away from the home network for a long time it must still be possible to manage him in a secure way without an HTD. Consequently, there is a need to decentralize the functionality of an HTD. To perform the AS method without an HTD we extend the basic AS method and use mix nodes.

Mix nodes was originally proposed by Chaum (1981) and can be realized by a special network station, which collects a number of messages of equal length from many different senders, discards repeats, changes their encoding and forwards the messages to the recipients in a different order. The technique of mixes is based on public key cryptography and provides unlinkability of sender and receiver.

5 ANONYMOUS SUBSCRIBER METHOD IN UMTS

For most of the time we can expect that most of the users are roaming in the vicinity of their homes (usually at home or at work) and are reachable in this limited area. The AS method plus an HTD can manage such subscribers in a trustworthy and efficient way (Kesdogan et al., 1995). If the mobile user is outside the home network domain it is desirable to find out the current pseudonym used and the location of the user through the nearest database. One way to decentralize the functionality of a trusted environment could be to define a trusted third party with the same functionality as an HTD, but serving a number of subscribers and controlled only by a third party organization which knows only the current pseudonym of a user, with the network provider only knowing the location of the pseudonym. Therefore, unless the third party and the network provider cooperate the privacy of the user is protected. However, any solution involving a trustable organization suffers from the difficulty of how to evaluate the offered security level. An organization is only as secure as its staff is trustworthy. Therefore, we introduce an approach based on mixes enabling the subscriber to control his/her own data.

We extent the classical MIX networks as described in (Chaum, 1981), (Pfitzmann, 1987), (Pfitzmann, 1991) and assume them to be capable to deal with a flag "Time Stamp (TS)" . If the input message to a mix node includes the TS flag in combination with an address, e.g. (TS=1, HA_B), the mix node will automatically generate a digitally signed message with the arrival time of the input message and will send this message to the specified address.

5.1 Registration for a Call Setup

MS_B roams in an area which is managed by a foreign network operator with the network number FNN (Foreign Network Number). In order to hide the actual position from this network provider MS_B registers himself via the mix nodes MIX_1 to MIX_3. The registration process starts by calculating* a message [HA_B, {HA_B, ID_7}] to the foreign network:

$$\{HA_B, ID_7\} := AMIX_3, c3(AMIX_2,(TS=1, HA_B), t_A, \\ c2(AMIX_1, (TS=1, HA_B), t_A, c1(t_A,(TS=1, HA_B), HA_B, FNN, ID_7, call\_setup) \quad (1)$$

$$[HA_B, \{HA_B, ID_7\}] := AMIX_1, c1(AMIX_2, \\ c2(AMIX_3, c3(FNN, anonymous\_registration, HA_B, t_A, \{HA_B, ID_7\}) \quad (2)$$

c1 through c3 are the public keys and $AMIX_1$ to $AMIX_3$ are the addresses of the mix stations MIX_1 through MIX_3, respectively. FNN is the Foreign Network Number. anonymous_registration, and call_setup should be standardized UMTS messages. HA_B is the well-known Home Address of MS_B, t_A is a time stamp and holds the expiration date of the covered message {HA_B, ID_7}. ID_7 is the current pseudonym which is rather long (e.g. 50 to 100 Bits) to avoid multiple selection of the same number from several mobile stations.

As shown in Fig. 3 the covered message [HA_B, {HA_B, ID_7}] is transmitted to the first mix MIX_1 (1). MIX_1 decrypts the message using its private key and finds the next hop address MIX_2, and so on. After these decryption operations the last mix transmits the message to the foreign network with the address FNN. We assume that a number of covered messages from

*For the sake of simplicity we do not include random numbers in the message. The exact calculation procedure of the message can be found in (Chaum, 1981), (Pfitzmann, 1987), (Pfitzmann, 1991)

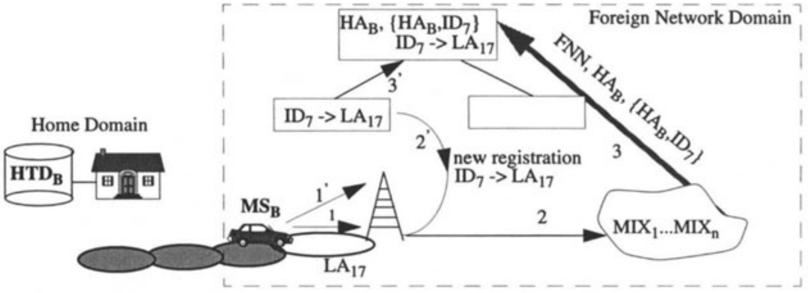

Figure 3 Anonymous registration.

mobile users are "mixed" through the MIX-Network at the same time, otherwise a backward revelation would be possible for the network operator. Receiving the message this network discovers (through the signalling message anonymous_registration) that this is a request from an anonymous registration of the mobile user with the international number HA_B and forwards the covered information $\{HA_B, ID_7\}$ to the root node (3). The network stores it until the message expires. In parallel to the covered registration (1 to 3) MS_B registers himself with the foreign network with the chosen pseudonym ID_7 and the current location area identifier LA_{17} (1'-3'). The covered information $\{HA_B, ID_7\}$ in combination with the well-known address of MS_B is a completely different entry for the network provider than the entry (ID_7 -LA_{17}).

5.2 Registration for Location Management

After this registration MS_B is able to roam in the foreign network area and use the pseudonym ID_7 for registration and location update (see Fig. 4): MS_B updates its location information from LA_{17} to LA_{18} using the pseudonyme ID_7 (1). ID_7 is known to the system and the associated location information will be updated. Managing the user with his/her pseudonym nobody is able to locate the subscriber B, only the pseudonym ID_7.

5.3 Mobile Terminated Call Setup

If a user A, located within the area of the foreign network, wants to communicate with mobile subscriber B and dials the HA_B, the foreign network initiates a network search for an entry HA_B. Upon detection of this entry (here in root node) it transmits the covered message of B to the specified mix node, e.g. MIX_3 (see Fig. 5). The mix nodes decipher the covered message and check the expiration time t_A until the last mix node finds the message "FNN, HA_B, ID_7,

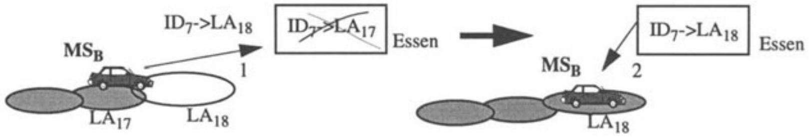

Figure 4 Location update

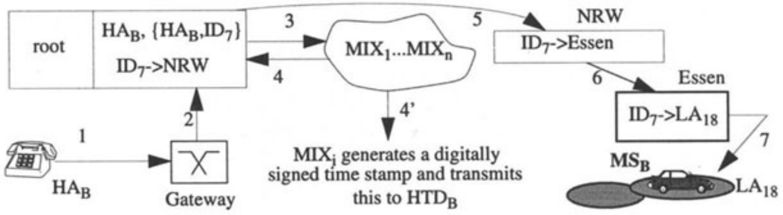

Figure 5 Mobile terminated call setup.

call_setup". This message will be transmitted to FNN. In the meantime, or subsequently, the mix nodes generate a message with the arrival time of the input message digitally signed and transmit it to HA_B (4'), as the TS flag is set to 1.

With the information "HA_B, ID_7, call_setup" the foreign network is able to start the sequence of location processes (5, 6 and 7). The MS_B stores the receiving time of the call_setup message. Consequently, two information are stored:

1. HTD_B stores the time stamp messages of the mix nodes.
2. MS_B stores the start time of the received mobile terminated calls.

Both information are needed to discover possible misuse by the foreign network.

5.4 Security Aspects of the new method

The covered message $\{HA_B, ID_7\}$ can be used by the foreign network only once because the mix nodes ignore repeated messages to prevent replay attacks. With the help of the time messages stored in HTD_B and in MS_B the user is able to audit the calls and to discover possible misuse by the foreign network provider. Frequent changes of the pseudonym will increase anonymity. The subscriber is able to determine the frequency of pseudonym changes by selecting an appropriate t_A. The covered message $\{HA_B, ID_7\}$ is only valid for the given time t_A and must then be renewed. Every new covered message including the expiration time t_A must be transmitted securely via mix nodes to the foreign network. This message must be more than 600 bits long, as encryption with an asymmetric cryptosystem like the RSA will not work properly otherwise. Consequently, the frequency of pseudonym changes is limited due to the limited bandwidth on the air interface. The trade-off between anonymity and costs must be discussed, but the pseudonym should be changed at least after every call.

6 APPLICATION OF THE AS-METHOD IN UMTS USING X.500

UMTS mobility management procedures require the existence of a distributed database maintaining service profiles, location and routing information, terminal profiles etc. The actual location of the data is assumed to be transparent to the user of the database. Even though UMTS is conceptually based on Intelligent Network concepts, the current IN CS-1 does not cover the required functionality for third generation networks. An example is the missing interaction between IN database nodes (so called Service Data Points, SDPs), which results in a non-transparency of the data distribution. To solve this problem improvements for the next IN capability set CS-2 have been made to include SDF-SDF interactions, but also the X.500 Directory service has been suggested as a major candidate for the internal strucutre of the UMTS distributed data base (RACE D733, 1995). After providing an overview of the Directory we therefore discuss the application of the AS-method in an X.500 based mobility management.

6.1 The X.500 Directory Service

This section is only intended to provide a very condensed overview of the relevant functionality of the X.500 Directory Service (DS); those who have a deeper interest in the directory's functionality should refer to e.g. (Chadwick, 1994) or the original standard (ISO 9594, 1993).

The DS provides a uniform naming scheme for and information about a network's resources (including e.g. hosts, processes, devices and human users). In terms of the DS, these resources are referred to as Objects. Usually, the DS is described as a - highly distributed - Client-Server System. This is characterized by a typically small number of hosts (the servers, the Directory System Agents (DSA)) providing callable services to the other hosts of the system (the clients, the Directory User Agents (DUA)). Fig. 6 shows the general model of the DS.

A Name is assigned to every object. This name is called Relative Distinguished Name (RDN). Every RDN is non-ambiguous relative to its immediate superior. The sequence of RDNs of an object plus those of its superiors forms the Distinguished Name (DN) of this object. The DN is globally unambiguous. The directory also provides for one kind of alternative names, called Aliases. They will prove crucial for the purpose of this paper. Every object is represented by an Entry, the totality of entries forms the Directory Information Base (DIB). An object's name and the information stored in an entry are composed of Attributes, which are tuples <AttributeType, AttributeValue>. Typically, the DIB is structured in a tree-shaped way; the Directory Information Tree (DIT), thus reflecting hierarchical relations between objects. Every DSA holds data about a subset of objects and has Knowledge about objects known by other DSAs (to provide for distributed operations). Knowledge is realized through References to other DSAs. The directory's Schema specifies the structure of the DIT, defines Object Classes (e.g. Country, Organization), Attribute Types (e.g. country name or telephone number) and Attribute Syntaxes (e.g. printable string or numeric string) permitted. The schema is composed from a number of Subschemas each valid within one particular management domain. The attribute type indicates the class of information given by that attribute. An object class definition specifies a set of mandatory and optional attributes for an entry of a given class.

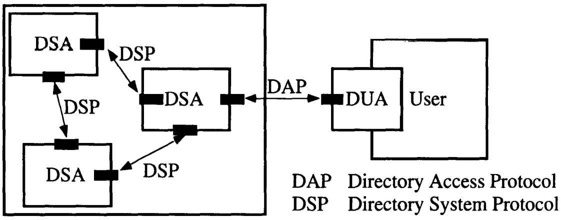

Figure 6 The general Directory model.

From an organizational point of view, the DS is hierarchically subdivided into subdomains, each of which is administered and managed by an Administrative Authority. It is this authority's task to assign names and to specify its subdomain's subschema.

6.2 X.500 to support anonymous mobility management operations

The basic idea is the use of the following UMTS numbers and identities as DNs (see also Fig. 7):

- IMUN: The International Mobile User Number is a unique identifier for a UMTS user and will be structured according to the numbering plans for ISDN (E.164) and UPT (E.168). The X.500 entry is an Alias entry referencing the internally used number of the user, the International Mobile User Identity (IMUI).
- IMUI+SI: UMTS services are identified by a Service Identifier (SI). A UMTS user may register with different services at different terminals (depending on his/her subscription). The IMUI is chosen as a distinguished name and the corresponding entry additionally holds attributes for subscription and general service information. The subscribed services are held in a subordinate entry with RDN SI. Thus, this entry is uniquely identified by IMUI+SI. In its other attributes this entry holds the detailed information of that service (ServiceProfile e.g. QoS parameter, accounting information), a reference to the terminal (DI+TMTI+TMUI, see below) where the user is currently registered for SI, and finally the entry includes information about the user status US, i.e. whether or not (s)he currently accepts incoming service requests. To achieve anonymity of the current location, the location information DI+TMTI+TMUI in the IMUI+SI entry is hidden from the network operator and is stored in an encrypted form (i.e., {DI+TMTI+TMUI}).
- DI+TMTI: The Temporary Mobile Terminal Identifier (TMTI) is chosen by the network operator upon domain update or when the terminal is registered the first time. Using a combination of the TMTI and the Domain Identity (DI) yields a unique identifier for a terminal. Thus, DI+TMTI will be used as the distinguished name for the terminal entry. The terminal entry includes attributes describing the terminal capabilities, the routing information (MTRN, Mobile Terminal Roaming Number), and the Location Area Identifier (LAI) required to page the terminal. To enable anonymous mobility management operations the user registrations at a terminal are not referenced directly by their IMUI. Instead, an encrypted pseudonym {TMUI} of the TMUI (Temporary Mobile User Identity) is used. The TMUI is a pseudonym of the IMUI+SI used for the interactions between terminal and network to save bandwidth on the one hand and to increase privacy on the other. To realize

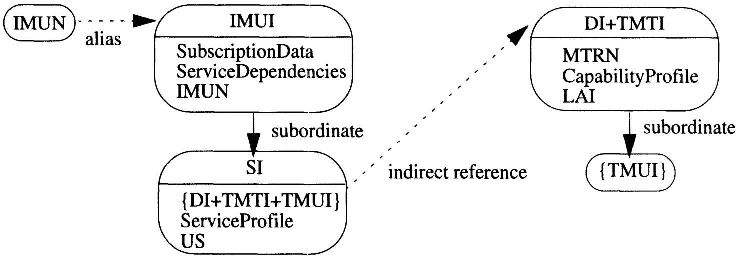

Figure 7 Structure of the Directory entries to support AS.

anonymity this identity TMUI is randomly chosen and encrypted, {TMUI}, by the terminal itself rather than by the network. The terminal transmits the {TMUI} via MIXes to a DUA which requests the Directory to update the IMUI+SI entry.

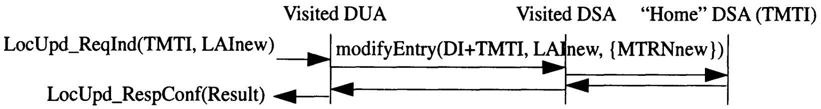
Visited DUA
Visited DSA
"Home" DSA (TMTI)
LocUpd_ReqInd(TMTI, LAInew)
modifyEntry(DI+TMTI, LAInew, {MTRNnew})
LocUpd_RespConf(Result)

Figure 8 Intra-domain location update.

Fig. 8 and 9 sketch the sequence charts for X.500 based mobility management procedures using the AS method. In case of an inter-domain update (Fig. 9) the terminal has to transmit the new DI+TMTI and {TMUI} identifier via MIXes to the Directory where the update of the IMUI+SI entry is performed. The data required for mobile terminated calls are obtained by following the entry dependencies in the DIT: IMUN +SI -> IMUI + SI -> DI+TMTI -> (MTRN, LAI).

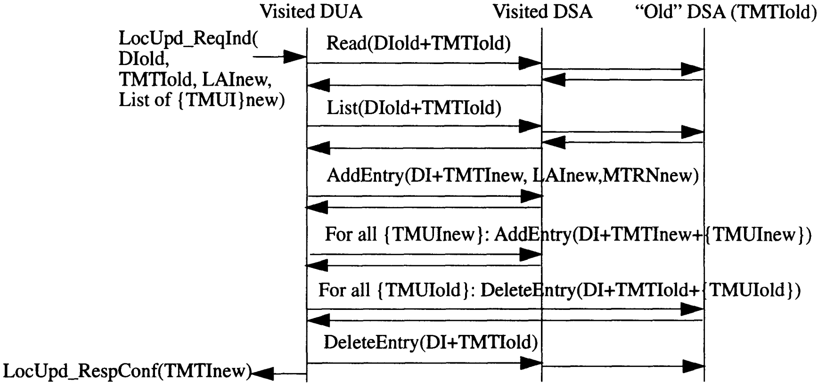
Visited DUA
Visited DSA
"Old" DSA (TMTIold)
LocUpd_ReqInd(DIold, TMTIold, LAInew, List of {TMUI}new)
Read(DIold+TMTIold)
List(DIold+TMTIold)
AddEntry(DI+TMTInew, LAInew,MTRNnew)
For all {TMUInew}: AddEntry(DI+TMTInew+{TMUInew})
For all {TMUIold}: DeleteEntry(DI+TMTIold+{TMUIold})
DeleteEntry(DI+TMTIold)
LocUpd_RespConf(TMTInew)

Figure 9 Inter-domain location update.

7 CONCLUSION

This work presented the AS-Method for UMTS, achieving privacy without an HTD. Using this method location management can be performed in an efficient way. We have discussed how to integrate the AS method into UMTS and how to apply it the X.500 directory service.

8 ACKNOWLEDGMENTS

This work is partially funded by the "Deutsche Forschungsgemeinschaft"
(grant no. Sp 230/9-2) and by the "Gottlieb Daimler und Karl Benz Stiftung".

9 REFERENCES

Armbrüster H. (1995) The Flexibility of ATM: Supporting Future Multimedia and Mobile Communications. *IEEE Communications Magazine*, February, 76-84.

Bar-Noy A., Kessler I., Sidi M. (1995) Mobile Users: To update or not to Update. *Wireless Networks*, July, 175-86.

Chadwick D. (1994) Understanding X.500 - The Directory. *Chapman & Hall.*

Chaum D. (1981) Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM,* 24/2, 84-8.

Farber D.J., Larson K.C. (1975) Network Security Via Dynamic Process Renaming; *Fourth Data Communication Symp.*, Quebec City, Canada , Oct., 8-13–8.

Fasbender A., Hoff S., Pietschmann M. (1995) Mobility Management in Third Generation Mobile Networks. *Proc. of the IFIP TC 6 Workshop "Personal Wireless Communications".*

Federrath H., Jerichow A., Kesdogan D., Pfitzmann A. (1995) Security in Public Mobile Communication Networks. *Proc. of the IFIP TC 6 International Workshop on Personal Wireless Communications*, 105-16.

ISO 9594 (1993) International Organization for Standardization: Information Technology - Open Systems Interconnection - The Directory, Part 1 - 9.

Jabbari B.: *Intelligent Network Concepts in Mobile Communications*; IEEE Communications Magazine, February 1992, pp. 64-69.

Karger P.A. (1977) Non-Discretionary Access Control for decentralized Computing Systems. Master Thesis, *MIT, Laboratory for Computer Science, Report MIT/LCS/TR-179.*

Kesdogan D., Federrath H., Jerichow A. and Pfitzmann A. (1996) Location Management Strategies increasing Privacy in Mobile Communication Systems; accepted for *IFIP SEC 96, 12th International Information Security Conference.*

Kesdogan D., Fouletier X. (1995) Secure Location Information Management in Cellular Radio Systems. *IEEE Wireless Communication Systems Symposium WCSS 95*, New York, 35-40.

Madhow U., Honig M.L., Steiglitz K. (1994) Optimization of Wireless Resources for Personal Communications Mobility Tracking. *Proceedings of the IEEE Infocom.* June, 577–84.

Pfitzmann A., Pfitzmann B., Waidner M. (1991) ISDN-MIXes: Untraceable Communication with Very Small Bandwidth Overhead. *Proc. IFIP/SEC 91*, Brighton, 245-58.

Pfitzmann A., Waidner M. (1987) Networks without User Observability. *Computers & Security*, 6, 158-66.

Pfitzmann A. (1993) Technischer Datenschutz in öffentlichen Funknetzen. *DuD*, 17/8, 451-63.

RACE 1043 (1991) Final Report on Fixed Network aspects in UMTS. Issue 2.0, *CEC Deliverable*, No.: 43/RNL/FN12/DS/A/067/b1.

RACE D731 (1994) Mobile Communications: General Aspects and Evolution. Issue E, *RACE Consensus Management R2083.*

RACE D733 (1995) Mobile Communications: Common Network Aspects.

Rahnema M. (1993) Overview of the GSM System and Protocol Architecture. *IEEE Communications Magazine*, April, 92-100.

Rapeli J. (1995) UMTS: Targets, System Concept, and Standardization in a Global Framework. *IEEE Personal Communications Magazine*, February, 20-8.

Spaniol O., Fasbender A., Hoff S., Kaltwasser J., Kassubek J. (1995) Impacts of Mobility on Telecommunication and Data Communication Networks. *IEEE Personal Communications Magazine*, October, 20–33.

Wang J.Z. (1993) A Fully Distributed Location Registration Strategy for Universal Personal Communication Systems. *IEEE Journal on Selected Areas in Communications*, August, 850-60.