TMSI Allocation Mechanism Using a Secure VLR Authorization in the GSM System

Mi-Og Park[1], Dea-Woo Park[2], and Sang-Geun Kim[1]

[1] Division of Computer Engineering, Sungkyul University, San 142-7, Manan-gu, Anyang 8-dong, Anyang-city, Gyeonggi-do, Korea 430-742
Mopark777@hanmail.net, Sgkim@sungkyul.edu
[2] Department of Computer Science, Soongsil University, Sangdo-dong 511, Donggak-gu, Seoul, Korea 156-743
Prof1@hanmail.net

Abstract. GSM is the most popular standard for mobile phones in the world. In spite of the tremendous market growth, however, the GSM system has the fatal security problems in TMSI allocation protocol. These problems are right user authentication and location privacy. In this paper, we propose the secure TMSI allocation mechanism using the certification concept to solve these problems. The proposed mechanism provides partial anonymity, which has been rarely provided in the other approaches. Also we propose the modified mechanism to reduce TMSI allocation procedure without changing of the architecture of the original GSM system.

1 Introduction

The Global System for Mobile Communications (GSM) is the most popular standard for mobile phones in the world. GSM service is used by over 1.5 billion people across more than 210 countries and territories. The ubiquity of the GSM standard makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world. GSM is an open standard which is currently developed by the 3GPP[1]. Security in GSM consists of the following aspects: subscriber identity authentication, subscriber identity confidentiality, signaling data confidentiality, and user data confidentiality. The subscriber is uniquely identified by the International Mobile Subscriber Identity(IMSI). This information, along with the individual subscriber authentication key Ki, constitutes sensitive identification credentials analogous to the Electronic Serial Number (ESN) in analog systems such as AMPS and TACS. The design of the GSM authentication and encryption schemes is such that this sensitive information is never transmitted over the radio channel. Rather, a challenge-response mechanism is used to perform authentication. The actual conversations are encrypted using a temporary, randomly generated ciphering key (Kc). The Mobile Station (MS) identifies itself by means of the Temporary Mobile Subscriber Identity (TMSI), which is issued by the network and may be changed periodically for additional security[2].

When the MS roams from one place to another, it is verified by using these security functions. However, GSM has the major security weakness during this procedure. The fatal problem is that anyone can listen an authentication parameter IMSI, which is uniquely identified a MS. In order to solve the problems with the TMSI allocation protocol in GSM, a lot of mechanisms have been proposed [3][4][5][6][7]. The most common mechanisms for secure TMSI allocation use basically the encryption between the VLR and the HLR. And also there are the many mechanisms that use the VLR authorization, which means that the VLR instead of the HLR authenticates the legality of the MS. In this paper, our mechanisms basically use the security functions, too. However, our mechanisms additionally provide the more many advantages than the existed ones.

The rest of the paper is organized as follows: First, we describe the TMSI allocation protocol defined in GSM. Then, we briefly describe the security of GSM e.g., user authentication and data confidentiality and the problems with TMSI allocation protocol in GSM. The main focus of the paper is Section 3, which propose the secure TMSI allocation protocol to solve the problems addressed above. In Section 4 and 5 we explain the main features and cryptanalysis about the proposed mechanism. We finally conclude this paper with a brief summary.

2 TMSI Allocation in GSM

2.1 Security Functions: Authentication and Confidentiality

In the GSM network, the subscriber is initially registered in the HLR with a unique identity, IMSI, and obtains one secret key Ki from the AuC(Authentication Center) during the registration process. HLR is a database used for mobile information management. All permanent subscriber data are stored in this database. The VLR is the database of the service area visited by an MS. Two location databases play important roles in subscribers' registration and authentication[8].

• User Authentication

Authentication is initiated by the fixed network, and is based upon a simple challenge-response protocol. When a MS attempts to access the system, the network issues it a 128-bit random challenge RAND. The MS computes the 32-bit signed response (SRES) based on the encryption of the random number RAND with the authentication algorithm (A3) using the individual subscriber authentication key Ki. The key Ki is unique to the subscriber, and is shared only by the subscriber and an authentication center, which serves the subscriber's home network. The value SRES computed by the MS is signaled to the network, where it is compared with a precomputed value. If the two values of SRES agree, the mobile subscriber has been authenticated, and the call is allowed to proceed. If the values are different, then access is denied. The subscriber authentication key is never transmitted over the

radio channel. It is present in the subscriber's SIM, as well as the HLR and VLR databases[9][10].

• Data Confidentiality

The same mechanism is also used to establish a cipher key Kc for encrypting user and signaling data on the radio path. This procedure is called cipher key setting in [3]. The key is computed by the MS using a one-way function A8, again under control of the subscriber authentication key, and is pre-computed for the network by the authentication center, which serves the subscriber's home network. Thus at the end of a successful authentication exchange, both parties possess a fresh Kc. The Kc is used to encrypt and decrypt the data between the MS and the VLR. The pre-computed triple (RAND, SRES, Kc) held by the fixed networks for a particular subscriber is passed from the home network's authentication center to visited networks upon demand. The challenges are used just once. Thus the authentication center never sends the same triple to two distinct networks, and a network never reuses a challenge.

In a similar manner to the authentication process, the computation of the ciphering key takes place internally within the SIM. Therefore sensitive information such as the individual Ki is never revealed by the SIM. Encrypted voice and data communications between the MS and the network are accomplished through use of the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the A5 and the Kc.

2.2 TMSI Allocation

The TMSI allocation allows mobile subscribers to originate calls and update their location without revealing their IMSI to an eavesdropper on the radio path. It thus prevents location tracing of individual mobile subscribers by listening to the signaling exchanges on the radio path. All mobiles and networks must be capable of supporting the service, but its use is not mandatory.

• TMSI Allocation Protocol and Its Problems

The TMSI updating mechanism functions in the following manner. For simplicity, assume the MS has been allocated a TMSI, denoted by $TMSI_o$, and the network knows the association between $TMSI_o$ and the subscriber's IMSI. The MS identifies itself to the network by sending $TMSI_o$. Immediately after authentication, the network generates a new TMSI, denoted $TMSI_n$, and sends this to the MS encrypted under the Kc as described in the above section. Upon receipt of the message, the MS deciphers and replaces $TMSI_o$ by $TMSI_n$[10].

Since GSM does not adopt ciphering mechanism between the VLR and VLR/HLR, an eavesdropper can monitor the physical channel that connects to the HLR. Also he can eavesdrop MS's location updating and user authentication information. These drawbacks of GSM enlarge the possibility of the privacy violation on users. It is found that the TMSI allocation protocol has some problems and weak-

nesses as follows[8]. The most important problem is the exposure of the IMSI and some other things are weakness.

• When the VLR updates the location of the MS, the IMSI is exposed and delivered throughout the network without any protection. This is the big problem in user authentication protocol.

• Mutual authentication mechanism between the MS and the VLR isn't provided. The GSM system only provides unilateral authentication for the MS. Using the challenge and response mechanism, the identity of a MS is verified. However, the identity of the VLR cannot be authenticated. It is therefore possible for an intruder to pretend to be a legal network entity and thus to get the MS' credentials.

• The VLR must turn back to the HLR to make a request for another set of authentication parameters when the MS stays in the VLR for a long time and exhausts its set of authentication parameters for authentication. There is bandwidth consumption between the VLR and the HLR.

• Every MS in the VLR has n copies of the authentication parameters. The parameters are stored in the VLR database, and then space overhead occurs.

• Authentication of the MS is done in the VLR and this must be helped by the HLR of the MS for each communication.

• When a user roams to another VLR, the location is updated by sending IMSI to the new VLR while the old VLR is not accessible and no correct subscriber data is available. It is possible that an unauthenticated third party may eavesdrop on the IMSI and identify this mobile user.

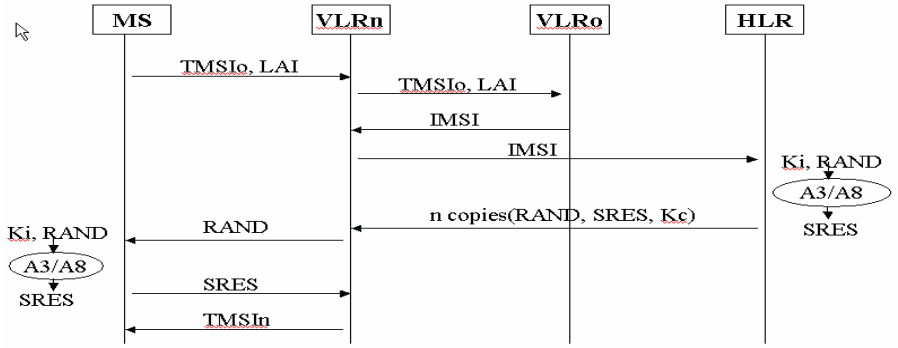

Fig. 1. TMSI Allocation Protocol and Security Functions

3 Secure TMSI Allocation Protocol

3.1 Basic Principles

The proposed mechanism will achieve the following main design objectives: secure user authentication, location privacy, partial anonymity, secure distribution of IMSI, the VLR authorization, and secure communication between the VLR and the HLR. Also the proposed mechanism has the following additional objectives: mutual au-

thentication, reduction of the stored space in the VLR, and reduction of bandwidth consumption between the VLR and the HLR.

• The generation method of TID

Our mechanism provides the partial anonymity capability. However, the most common papers seldom provide user's anonymity[3][8]. In this paper, partial anonymity has literally the meaning that guarantees partially user anonymity in the TMSI allocation protocol. In order to provide partial anonymity, the proposed mechanism uses a MS's temporary identity (TID). The usage of a TID can also avoid the location tracking. The old VLR transmits the TID instead of the IMSI to the new VLR before completing verification of the new VLR by the HLR. The new VLR can acquire the IMSI only after being completed verification by the HLR. So user's anonymity is provided until the new VLR is authenticated by the HLR.

The TID is mapped by one-to-one with the IMSI. So the TID must be unique in the HLR of the MS as an additional parameter to authenticate the MS instead of the IMSI. The relation between the TID and the IMSI is kept secretly only by the HLR and the MS. But, the parameter TID itself is public information. And only the HLR can generate user's new TID. User can take together new TID during the registration process that he/she obtains the Ki and the IMSI. The HLR gives the new VLR authorization to authenticate the MS. But, the new VLR processes authentication of the MS without knowing the Ki of the MS. If the MS stays in the coverage of its new VLR for a long time, the new VLR does not go back to the HLR to require another set of authentication triple (RAND, SRES, Kc) to authenticate the MS.

• The generation method of the Certificates

The VLR authorization means the capability that the new VLR instead of the HLR authenticates the MS. For this capability, the new VLR must have a temporary secret key shared between itself and the HLR. We notate this key as a TKi. The new VLR only uses the TKi of the HLR given with its generated RANDj for each call to compute the SRES and then identifies the MS, where RANDj is a random number generated by the new VLR in the subsequent calls. Only one RANDj is generated by the new VLR for each jth call no matter how long the MS stays in the coverage of the new VLR. This operation will be done only once in the first call when the MS visits at the new VLR.

Table 1. Notations

T1	Timestamp generated by the MS
T2	Timestamp generated by the new VLR
RAND1, RANDv	Random numbers generated by the new VLR
RAND	Random number generated by the HLR
K_{VH}	Secret key shared between the HLR and the VLR

In order to endow the new VLR with MS authorization, the HLR requires legality of the new VLR. We use the certification concept to check legality of the new VLR. The HLR generates the certification of the VLR e.g., $Cert_{HM}$ after performing authentication of the VLR. In our paper, the certifications ($Cert_{HM}$, $Cert_{MS}$, and $Cert_{VLR}$) are different from the general certification in a public key infrastructure

cryptosystem. The MS computes the certification of the MS, $Cert_{MS}$ through A3 using (Ki, T1) to prove itself to the HLR. In order to obtain the capability that authenticates the MS from the HLR, the new VLR should be strongly verified by the HLR. The compositions of the VLR certification e.g., $Cert_{VLR}$ are K_{VH}, RANDv, T1, and T2. $Cert_{VLR}$ is generated by running A3 using K_{VH} and X3, which is produced by computation of XOR with T1, T2, and RANDv.

Table 2. Certification Generation Method

$Cert_{MS}$	A3(Ki, T1)
$Cert_{VLR}$	A3(K_{VH}, X3)
$Cert_{HM}$	A3(Ki, T1) ‖ A3(Ki, RAND)

The HLR computes the certification of the new VLR, e.g., $Cert_{HM}$ through A3 using (Ki, T1) and (Ki, RAND) to prove the fact that the new VLR is a genuine entity to the MS. The temporary key between the MS and the new VLR, TKi is computed by running A3 with Ki and the result value after doing XOR RAND and T1.

3.2 TMSI Allocation Procedure

The procedure for the proposed TMSI allocation mechanism is following as:

Step 1) The MS sends TMSI, LAI, $Cert_{MS}$, TID, and a time-stamp T1 to the new VLR. T1 enables to authenticate the new VLR and it prevents from replay attack.

Step 2) After receiving TMSI and LAI, the new VLR forwards TMSI and LAI to the old VLR to obtain the MS's TID.

Step 3) The old VLR sends the TID instead of IMSI to the new VLR after searching for the TID corresponding to TMSI and LAI in its database. If there is no TID corresponding to the TMSI and LAI, then the session will be terminated.

Step 4) The new VLR generates RANDv and timestamp T2. And then the VLR computes $Cert_{VLR}$ according to the certification generation method. After that, the VLR transmits the TID along with the identity of the VLR, e.g., VLR_{ID}, T1, T2, RANDv, $Cert_{MS}$ and $Cert_{VLR}$ to the HLR. RANDv and T2 are used to authenticate the VLR itself to the HLR. RANDv may be encrypted using A5 with Kvh for the secure transaction, since the RANDv is used as the parameter to authenticate the VLR in the HLR.

Step 5) Once receiving the parameters, the HLR checks if VLR_{ID} is a legal or not. If it is correct, then the HLR computes the X3 by using the transmitted T1, T2, and RANDv and does $Cert_{VLR}$' value to authenticate the VLR, since the HLR knows the shared key K_{VH} between the VLR and the HLR corresponding to the VLR_{ID}. If $Cert_{VLR}$' and $Cert_{VLR}$ are same, the HLR believes the new VLR is a genuine entity and computes TKi. And then the HLR computes Evh(IMSI, TKi) through A5 with a secret key K_{VH} using the TKi and the IMSI corresponded to the transmitted TID. At the same time, the HLR generates RAND and computes E_{HM}(RAND) using A5 and $Cert_{HM}$. Finally, the HLR transmits the identity of the HLR e.g., HLR_{ID}, T1, $Cert_{HM}$, E_{HM}(RAND), and E_{VH}(IMSI, TKi) to the new VLR.

Step 6) Once receiving the parameters, the new VLR extracts the IMSI and the TKi, since it can know the shared secret key K_{VH} by checking the HLR_{ID}. The VLR

generates the random number RAND1 to authenticate the MS. In the next call, the VLR should generate another random number. The VLR transmits T1, E_{HM}(RAND), RAND1, and $Cert_{HM}$ to the MS.

Step 7) Upon receiving the parameters, the MS first checks if T1 is the same as it was when last sent. If the result is valid, the MS computes $Cert_{HM}$' and then it compares the $Cert_{HM}$' computed by itself with the $Cert_{HM}$ received from the VLR. If two certification values are the same, the MS believes the new VLR and generates TKi after decryption E_{HM}(RAND). The MS continues through A5 using TKi and RAND1 as inputs to generate the SRES, which is then sent back to the new VLR.

Step 8) Once receiving the SRES from the MS, the new VLR computes the SRES' through A3 using TKi and RAND1 and compares the SRES' with the received SRES. If they are the same, the authentication of the MS is successful. Finally, the new VLR generates and transmits the new TMSI to the MS.

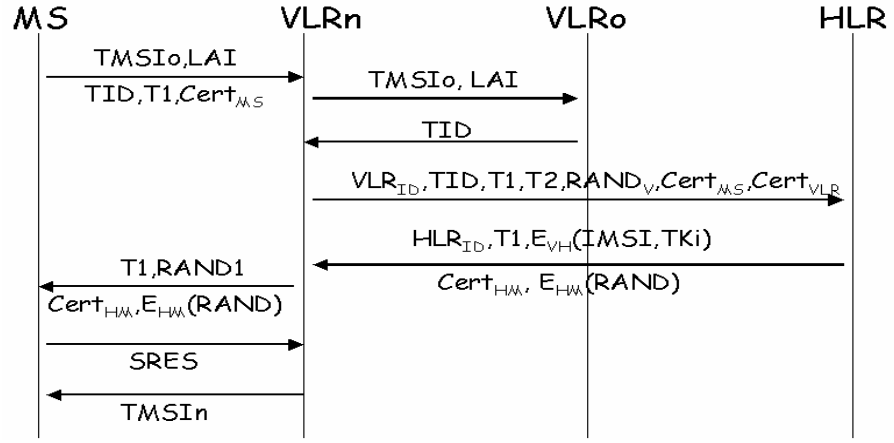

Fig. 2. Secure TMSI Allocation Procedure

3.2 The Reduction of Procedure

In order to reduce the numbers of the proposed procedure, we introduce the modification mechanism that changed the procedure of the first proposed mechanism. The basic concepts are the same as one of the first proposed mechanism. However, there is one different point in the procedure.

One difference is that steps 2 and 4 in the first mechanism are simultaneously performed in the second mechanism. So, steps 3 and 5 are automatically and simultaneously performed after being completed them respectively. That is to say, the new VLR immediately transmits the TID that is sent from the MS to the HLR after completing the 1st step without waiting for the transmission of the TID from the old VLR in the 3rd step because the new VLR already has the TID that sent from the MS in the 1st step. As a result of, steps 2 and 4 in the first mechanism become step 2 in the second one. And steps 3 and 5 in the first mechanism become step 3 in the second one.

4 Main Features

Our mechanisms provide the following features. So our mechanisms satisfy the design objectives. First, we explain the features that provided in only our mechanisms.

• The first user authentication and the second one: In step 3 of the first proposed mechanism, the new VLR can know that certain attack exists if the different TID is sent from the old VLR. Thus, the first proposed mechanism provides the first user authentication to authenticate simply the MS by the transmission of the TID in step 3. The second user authentication is provided in step 5, which is the core user authentication. In our second mechanism, the first user authentication and second one are provided in step 3. Steps 3 and 5 of the first mechanism belong to step 3 of the second mechanism because of the simultaneous processing character of the second mechanism. Thus the proposed mechanisms provide the feature that can authenticate the MS two times without the additional procedures.

• Partial anonymity: The conventional mechanisms don't provide almost partial anonymity. Our mechanisms provide the mobile user with partial anonymity by using a TID until the HLR of the MS authenticates the new VLR. The procedure to provide partial anonymity brings the effect to reduce encryption processing, since the parameter TID itself is the public information in our paper.

• Stronger VLR authentication: The proposed mechanisms provide the stronger VLR authentication. In the common mechanisms for the secure TMSI allocation, the original user authentication of the GSM system has been used to authenticate the new VLR by the HLR. That is to say, the HLR authenticates the new VLR by using the A3 with a Ki and a time-stamp T in the common mechanisms. However, in the system that the new VLR instead of the HLR authenticates the MS, it's necessary the more secure authentication function to authenticate the new VLR because the new VLR is responsible for the MS authentication. Our VLR authentication method is more secure for the additional VLR authentication parameters as described in section 3.

• Only VLR that is authenticated by HLR can use MS's IMSI: The conventional mechanisms and the original GSM system assume that the VLR is a legal entity. But, in this paper, the HLR believes the new VLR according to the verification result after authenticating the new VLR without any assumption. By the certification generation method of the new VLR, the HLR can authenticate securely the new VLR.

• Procedure reduction: The second proposed mechanism reduces from 8 to 6 steps for a new TMSI allocation and from 7 to 5 steps for the MS authentication in the new VLR because of the simultaneous processing of the second mechanism. So our mechanism can authenticate the MS and allocate the new TIMSI in shorter time. Also it reduced the total procedure without totally changing the original architecture of GSM.

The following items are features that have been provided in the most common approaches for secure TMSI allocation. Our mechanisms also provide the following features.

• Secure user authentication and location privacy: These are the most important objective. Our mechanism used the TID instead of the IMSI between the new VLR

and the old VLR. It is possible for any network entities including the new VLR to acquire the IMSI only after the HLR of the MS authenticates them. When the HLR transfer the IMSI to the new VLR, the IMSI is sent in the encrypted mode by using the shared secret key between the HLR and the VLR. Thus user authentication and location privacy are supported, since the value IMSI isn't exposed the unauthenticated entities.

• Mutual authentication between the MS and the VLR: The HLR generates the $Cert_{VLR}$ after authenticating the new VLR by the $Cert_{VLR}$. By verifying the $Cert_{VLR}$ transmitted from the HLR, the MS can ensure that it is communicating with a legitimate VLR.

• Reduction of bandwidth consumption: The HLR gives the VLR temporary secret key TKi to authenticate the MS. As long as the MS stays in the coverage area of the new VLR, the VLR can use the TKi to authenticate the MS for each call. Since the new VLR does not go back to the HLR to require another set of authentication triple, the signaling load is reduced between the VLR and the HLR.

• Reduction in the storage of the VLR database: The VLR only stores one authentication parameter instead of n copies (RAND, SRES, Kc) according to the principle of the reduction of bandwidth consumption.

• The application of the existed security: There is no any change in the original architecture in order not to lose simplicity and efficiency advantages of GSM, which is widespread in the world. The security of the proposed mechanisms is also still based on algorithms A3, A5 and A8.

• Authentication of the MS by the new VLR: Authentication of the mobile user is to be done by the new VLR instead of the HLR except the first call for the TMSI allocation, even though the VLR doesn't know the subscriber's secret key Ki.

The conventional approaches don't satisfy all our design objectives. And also the many approaches mostly change the original architecture of the GSM TMSI allocation protocol. Our mechanisms keep the advantage of not changing the architecture of the GSM system. Table 3 shows some approaches with the unchanged architecture. Lee et al. [8] proposed a mechanism that doesn't change the architecture. But, their mechanism doesn't provide mutual authentication between the MS and the VLR. The original GSM doesn't also support mutual authentication. Since the VLR doesn't ask the HLR for another set of authentication triple in Lee et al.'*s* and our mechanisms, the bandwidth consumption is less than that of the original GSM protocol. Because the VLR only requires storage of one copy of the authentication triple instead of n copies in Lee et al.'s and our mechanisms, the storage in the VLR can be saved.

The explained capabilities are concisely arranged in table 3. The followings are the meanings of the abbreviated words: PA: Partial anonymity, AI: Assignment of the IMSI, UAV: The use of IMSI after authentication the VLR, EVV: Encryption between the old VLR and new VLR, RBC: Reduction of bandwidth consumption, RSV: Reduction of storage in the VLR, RTP: Reduction of the total procedure, MAMV: Mutual authentication between the MS and the VLR, CAG: Change architecture of GSM. As shown in table 3, the common approaches have used encryption between the old VLR and the new VLR. Also they encrypted all parameters between the VLR and the HLR. However, the proposed mechanisms made to the

minimum the usage of encryption by applying it to the only parameters is in need of encryption.

Table 3. Comparison among TMSI allocation mechanisms

	GSM	Our mechanism	[8]	[7]	[11]
PA	N	Y	N	N	N
AI	VLR	HLR	VLR	VLR	VLR
UAV	N	Y	N	N	N
EVV	N	N	Y	Y	Y
RBC	N	Y	Y	N	Y
RSV	N	Y	Y	N	Y
RTP	-	N	Y	Y	N
MAMV	N	Y	N	Y	N
CAG	-	N	N	N	N

5 Cryptanalysis

Owing to the fact that we adopt the architecture of the conventional authentication in GSM, the security of the proposed mechanisms, which is the same as that of the existing authentication method in GSM, is based on algorithms A3, A5 and A8. In order to authenticate the legality of the new VLR and the MS, we add a time-stamp T1 and T2 to the TMSI allocation protocol. The T1 and T2 enhance the security of the proposed mechanisms against a replay attack. Although an attacker can intercept T1, T2, RANDv and $Cert_{VLR}$ and then forge the real VLR, the replay still cannot succeed because T1 and T2 are incorrect. The MS can also check if the T1 is the same as it was when sent the last time even if the fake VLR replays T1 and $Cert_{VLR}$.

The new VLR is verified in the MS by using the $Cert_{HM}$ that generated from the HLR. Nobody can forge it to fool others, since the secret key Ki is known only to the MS and the HLR. The proposed $Cert_{HM}$ and $Cert_{VLR}$ are made the stronger than the other certification mechanisms of the new VLR. Without the knowledge of Ki, $Cert_{HM}$ cannot be computed by anyone. Therefore, the security of the proposed mechanisms is based on Ki. For authenticating the MS, the new VLR only generates a different RANDj to compute the SRES for every jth call. The security here is based on the HLR giving the new VLR authorization to authenticate the MS. Nobody can suppose the value IMSI with the TID, since only the HLR knows the relation between the TID and the IMSI. Also there is no the exposure of the IMSI in wired channel, since the only authenticated VLR can use the IMSI and this VLR is transfer the IMSI in encryption mode.

6 Conclusions

In this paper, we have proposed new TMSI allocation mechanisms used the certification concept to solve the fatal problems of user authentication and location privacy in the GSM system. Besides, the proposed mechanisms provide partial ano-

nymity and stronger VLR authentication. The stronger VLR authentication is very important in the most common approaches for the secure TMSI allocation, which have used the way that the new VLR instead of the HLR authenticates the MS. In order to authenticate the MS by the new VLR instead of the HLR, the HLR must strictly authenticate the new VLR. Thus the stronger VLR authentication is needed. However, the most approaches have merely used the general user authentication of the original GSM system. Our mechanisms provide the more secure way to authenticate the MS by the new VLR, since our approaches provide the stronger VLR authentication by applying the certification as described above. Also our mechanism provides the reduction of the TMSI allocation procedure by doing simultaneously the procedure without changing the procedures of the original GSM system.

References

1. http://en.wikipedia.org/wiki/GSM
2. http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html
3. HARN, L. and LIN, H.Y: Modification to enhance the security of the GSM protocol, Proceedings of the 5th National Conference on Information security, Taipei, Taiwan, May. (1995) 416-420
4. Lee C.C., Hwang M.S., Yang, W.P.: Extension of authentication protocol for GSM. IEE Proceedings. Communications, Vol. 150, No.2, (2003) 91-95
5. AL-TAWIL, K., AKRAMI, A., and YOUSSEF, H.: A new authentication protocol for GSM networks, Proceedings of IEEE 23rd Annual Conference on Local computer networks(LCN'98), 21-30 (1998)
6. STACH, J.F., PARK, E.K., and MAKKI, K.: Performance of an enhanced GSM protocol supporting non-repudiayion of service, Comput. Commun., 675-680 (1999)
7. Molva, R., Samfat, D., Tsudik, G.: Authentication of mobile users, Network, IEEE Volume 8, Issue 2, (1994) 26 – 34
8. K. Chae and M. Yung (Eds.): WISA 2003, LNCS 2908, pp. 162.173, 2004. Springer-Verlag Berlin Heidelberg 2004, A Location Privacy Protection Mechanism for Smart Space
9. http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsmsecur.html
10. http://jya.com/gsm061088.htm
11. Chii-Hwa Lee, Min-Shiang Hwang and Wei-Pang Yang, Enhanced privacy and authentication for the global system for mobile communications, Wireless Networks 5 (1999) 231–243