JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 15, 471-484 (1999)

A Novel Application of the Phone Card and Its Authentication in Mobile Communications[1]

C. H. LEE[+], M. S. HWANG[*] AND W. P. YANG[++]
Department of Computer and Information Science
National Chiao Tung University
Hsinchu, Taiwan 300, R.O.C.
[+]*E-mail: chrissy@dbsun1.cis.nctu.edu.tw*
[++]*E-mail: wpyang@cis.nctu.edu.tw*
[*]*Department of Information Management*
Chao Yang University of Technology
Taichung, Taiwan 413, R.O.C.
E-mail: mshwang@dec8.cyut.edu.tw

The Subscriber Identity Module (SIM) is conventionally used in wireless communication systems. However, several limitations involving SIM significantly reduce public access in wireless communications. This study examined the feasibility of using public telephone cards in wireless communications. This novel application retains the merits of SIM. Among the relevent issues addressed are location tracking of the user, authentication of the phone card, and the billing scheme. Moreover, two implementations of phone card authentication are presented.

Keywords: authentication, billing system, location tracking, mobile communications, one-way function, phone card, public-key cryptography

1. INTRODUCTION

The Subscriber Identity Module (SIM) concept has been widely used in modern mobile communication systems. It serves as a means of security in terms of authenticating the user identity. Unauthorized charges to a user's account are, thus, prevented by means of its authentication process. Application of the SIM card to the mobile phone is exactly the same as the use of credit cards in our daily life. It signifies a personal account and is a proprietary object. To obtain the card requires registration and takes personal credits into account. The card is a prerequisite for conducting any transactions. A SIM card is portable and can be inserted into any mobile telecommunication equipment. Consequently, SIM cards can be applied in mobile equipment and network systems, thus allowing the user to roam from one place to another, with accurate charges to the designated account.

The SIM plays a major role in the security for both subscribers and networks [1-3]. Because the billing is associated with the SIM card rather than with any terminal or network equipment, the subscriber is not limited to using a particular mobile instrument. It can

Received May 6, 1997; accepted November 21, 1997.
Communicated by Jean-Lien C. Wu.
[1]Portions of this paper was presented at the 1997 The Seventh National Conference on Information Security, May, Taiwan, R.O.C.

be rented, borrowed, or shared between subscribers. Once the SIM card is removed from equipment, the billing scheme follows. The use of SIM facilitates more flexible applications using the same billing account. Notably, other equipment can replace a mobile station that fails. In addition, a user can select the best available equipment, e.g., borrow a more powerful mobile station in an urban area, use a handset in the countryside, or rent a car equipped with a vehicle-mounted station, all using his own SIM card. Moreover, the mobility of SIM is extended to earn the services transmitting through different systems using different radio techniques. Just as commercial credit cards can be used in available pay phones, SIM cards can function similarly in mobile equipment.

Nevertheless, as opposed to the merits and faults of a credit card, a SIM card has certain disadvantages in terms of public access. Registration and approval are required before a card can be issued. The need of a specified physical object also reduces the convenience and accessibility for public use of wireless communications in a flexible manner. Those who use wireless communications occasionally may wish to pay flexible and limited expenses at certain times and in certain places. Those who hope to reduce the risk of losing a personal SIM card may need more flexibility in using mobile phones. The circumstances described above point to the need for more versatile applications. Therefore, in this study, we examined the feasibility of using a phone card in public telephones for mobile communications.

Phone cards have been widely used in conventional telephone systems. It is common to purchase a phone card in advance and make phone calls using stationary public phones in the buildings or along streets. The novel application of phone cards in wireless mobile communication systems creates a new service for the phone cards. This new application of phone cards also provides another communications choice for users.

Herein, we present the idea of using a phone card as the public temporary SIM in mobile communications. Examples are also provided. Issues related to this phone card application, in which authenticating the card is the critical task, are addressed. Moreover, two implementations of the authentication process are presented along with operational considerations.

2. PHONE CARD APPLICATIONS

The phone card, a novel mobile phone application, is proposed to improve on and, in the same time, include the merits of SIM. The phone card provides users with a value-added alternative to SIM. The scenario is that a user purchases a phone card from a service provider just as he purchases a temporary SIM card, and he can then use any mobile phone at any place to originate calls and to receive calls, if needed.

The SIM card is generally manufactured in two different sizes: “full size”, or credit card size, and “plug in” size, which is approximately 25mm x 10mm. SIMs are much more sophisticated devices than smart cards typically used in pay phones. A SIM contains a microprocessor and a minimum of two Kbytes of Electrically Erasable Programmable Read Only Memory (EEPROM). A waiting period is necessary to process and issue a SIM card. A user is probably unable or unwilling to accept such a waiting period for subscribing to the service or obtaining a new reissued card. Following the waiting period, the user can purchase a phone card from an authorized company and use it as his temporary SIM to use any

mobile phone. On the other hand, it is possible that a SIM card may be lost or stolen. The result will be a large financial loss. However, a phone card may only contain a limited amount of monetary value, and the impact of loss can also be mitigated.

Some mobile communication users are frequent global travelers, and it is not convenient for them to carry their SIMs and handsets with them all the time. Users who need to use mobile phones without using their own SIMs and handsets could purchase phone cards for use as temporary SIMs and use any available mobile phones. Upon arrival at an airport, a user can rent a mobile phone as easily as renting a car. Then, upon their departure, the users return the equipment. Phone cards could be purchased at any authorized location or at phone-rental companies. Billing for using the phone cards would be automatically transferred to the card issuer.

Mobile phones will no doubt become increasingly popular and ubiquitous. Phone card applications would allow public access to mobile equipment, just as easily as to public phones. Therefore, problems associated with SIM card applications and processing could then be averted. Ultimately, the phone card could provide a more flexible alternative to SIM.

3. ARCHITECTURE OF WIRELESS MOBILE COMMUNICATIONS

The architecture of wireless mobile communications with phone cards is shown in Fig. 1. The architecture is similar to the general two-level hierarchical database structure of mobile communications, such as the North American IS-41 cellular standard [4] and the European GSM standard for mobile communications [5, 6], except adding the global location database called the Global Home Location Register (Global HLR).

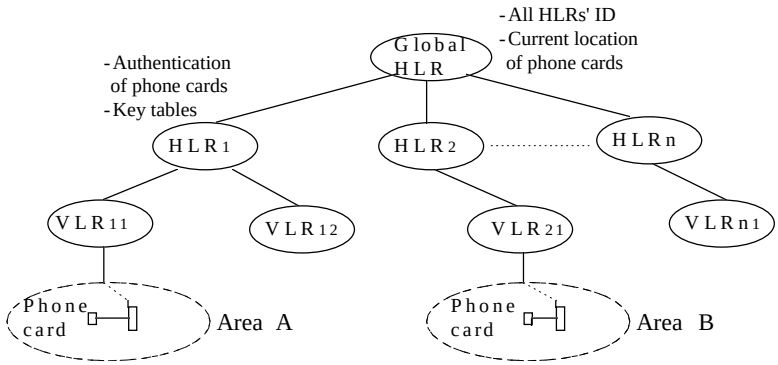

Fig. 1. Architecture of wireless mobile communication with phone card.

In Fig. 1, the solid lines represent the logical relationships of the databases. The Global HLR is a global database that stores information needed for the operations of phone cards in this system. The Home Location Register (HLR) is the location database system, which stores registration information for all issued cards. The Visitor Location Register (VLR) is the location database system, which stores the location information and billing

records for the cards. Information stored in the Global HLR at least consists of the look up tables of home domain's identities, i.e., the HLRs' identifiers (HLR.id), and the current locations of phone cards. All HLRs, which can be domestic or international ones, connect to the Global HLR. The Global HLR tracks the location of each user when he is roaming in different areas. For instance, the card holder can roam from Area A to Area B. When a call is delivered to a card holder, the central Global HLR can easily trace the exact location of this user, and the networks then can set up the communication trunk. A circumstance in which no Global HLR serves as a central information provider stipulates that (a) every HLR must handle location tracking for its cards, and (b) all HLRs must search for the card holder and can then receive the incoming call. This process subsequently makes the system more complicated and less efficient. For simplicity in this study, we adopt the central structure of the Global HLR. Since the mobility patterns of cardholders may be somewhat locality related, for more efficient performance, the database in the Global HLR could be distributed or replicated at several sites. However, this topic is beyond the scope of this study; further research will address data replication and performance evaluation in the phone card application.

Among the pertinent issues related to the use of phone cards are location tracking of users, authentication of phone cards, and a billing scheme for VLR [7]. The following sections describe location tracking and the billing scheme. Further details regarding how phone cards can be authenticated will be discussed as well.

4. LOCATION TRACKING OPERATION

There is no need for location tracking of a cardholder when the user makes an outgoing call. The system only needs to manage the authentication and the billing record for this phone card. On the other hand, location tracking is required when the network attempts to deliver a call to a cardholder who is using a specific mobile phone at a specific time. In the case of receiving a call, the authentication and billing processes are also needed if the payment policy is designed such that a wireless receiver pays the communication fee. Otherwise, authentication of the phone card and billing process are not required. Fig. 2 shows the process of location tracking of a phone card. If a cardholder wants to receive any incoming call in a visited area B, he has to register in this new area beforehand. He may insert the card in any mobile phone; then, he may either key-in his Personal Identifier (PID) or the PID will be automatically read from the card by the mobile phone to register in this VLR. The visited VLR21 passes his PID and related information of this mobile phone to the Global HLR to record the location of this specific PID using this specific mobile phone.

Whenever and wherever a Public Switched Telephone Network (PSTN) caller or another mobile caller originates a call to this PID from the PSTN (Steps 1 & 2) or other VLR, the dialed number is his PID. The network queries Global HLR for the location information about this PID. If Global HLR does not have any information about this PID, which implies that this PID has not been registered in the Global HLR or that this PID is an incorrect number, the network will reject the call request. Otherwise, the Global HLR will reply with the current location of this PID to network (Step 3). Then, the network will set up a trunk between the caller and callee (Step 4).

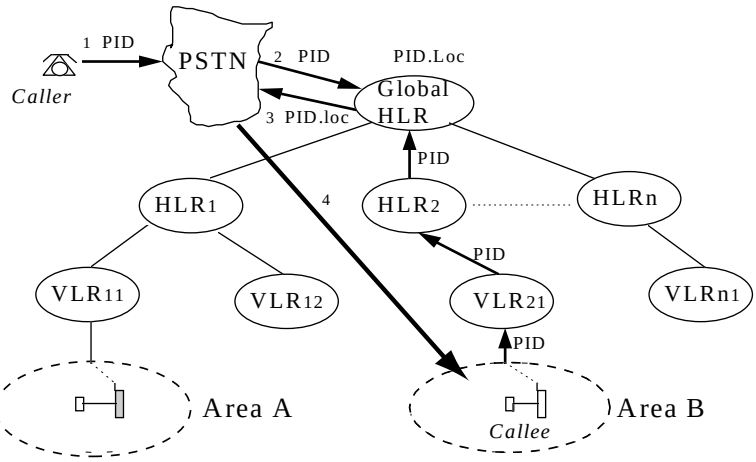

Fig. 2. Process of location tracking for a phone card.

The PID can be regarded as a virtual dialing number for a specific person or a specific card. According to the network operation policy or the authentication mechanism of the phone card, the PID can be either freely chosen by the card holder in the registration phase or assigned by the card issuer to represent the user's identity. In the one-way function approach described in this study, a freely chosen PID is adopted to authenticate the card. In the public-key cryptography approach, an assigned PID is used to authenticate the card. The format of the PID in the phone card is different from the dialing number when a SIM card is used. A network can easily distinguish between different types of requested services. On the other hand, card holder either (a) leaving another area or (b) desiring to cancel the registration of a mobile phone can insert the card into the mobile phone so that the deregistration process can be performed. Otherwise, the old location will still be tracked although it is no longer valid.

5. BILLING SCHEME

The phone card is a pay-first, service-later application. Periodically, the HLR/VLR of visited domain will bill to the home domain HLR of the phone card. Considerations regarding the design of this billing scheme must be addressed. The HLR issues phone cards and stores authentication keys in them. It keeps the necessary information for its phone cards and performs authentication whenever a phone card is used. The VLR verifies the phone card before service is launched. The general key format of the phone card can be shown as

HLR.id	Keys...	NB (or TU)

HLR.id denotes the global unique identifier of the home HLR that issues the phone cards. There are n keys generated by the HLR and stored in the card. NB represents the Number of Bills, and TU is the Time Unit for a call. Both NB and TU can be optionally included in the key format as the billing unit, where NB is used to charge by the number of calls and TU is used to charge by time. The fact that the phone card is an application in which the fee is first paid and the service is requested later accounts for why the visited VLR, which provides the service to a phone card user, bills the home HLR for its service.

The quota of phone use is managed using the keys. When a key has been used to authenticate a card, it is marked as "dirty" or scratched by the mobile terminal and cannot be read or used again. For each successful authentication of the card, the HLR updates the count data n using the one-way function approach or C using the public-key cryptography approach. Any unmatched count values (more or less) mean that the HLR has to reject the phone card. When a user uses a fake card which copies all data from a real one, the conflict in the count data can be detected soon after these two "identical" cards are used. Then, both the real and fake cards will be rejected by the system.

When the quota of the phone card is empty, this means that all the keys are used up and have been marked "dirty" or have been scratched on the phone card. Therefore, if any card is used in which the quota has been used up, the mobile phone can detect htis situation at once. Since the phone card does not have any more "clean" keys can be read and transferred by the mobile phone to the VLR, the mobile phone will immediately reject this card.

Due to the existence of different networks which have different rates for call services, the billing policy needs to be coordinated and determined by all associated network operators in advance. The charging components may be the VLR's service, the communication cost, the signaling cost, etc. Periodical billing records will be collected and analyzed by the HLR. The HLR will then distribute the fee to all the cooperating networks.

Two possibilities arise in which unauthorized charges are made from a visited HLR/VLR: (a) a visited VLR keeps the key of the phone card and reuses it, or (b) a VLR shares the key with other VLRs. Under such circumstances, the problem of replaying occurs, in which a key is reused more than once by a VLR or is shared by several VLRs. The authentication approaches proposed herein can eliminate such an occurrence.

Another possible scenario involving unauthorized charging is that a VLR may overcharge for a given call. If the HLR does not have any account data for the elapsed time of each call, the VLRs may modify the record of the call time and can then charge more. To accumulate the duration of a call by VLR is an uncertain factor for charging. However, the overcharging problem can be resolved by simply using the time unit assigned by the HLR in the card. It performs the authentication process again when a TU, i.e., the charging unit per time interval, expires. That is the reason why, in this study, our authentication approaches add the extra data of n and C in the two proposed implementations, respectively, to record the current call count, which indicates the number of time unit. Thus, the billing scheme herein is designed to charge by time units for each call, which forces key authentication to be performed again while the time unit expires.

6. AUTHENTICATION OF A PHONE CARD

6.1 Authentication Procedures

Confidentiality of radio transmission and authentication of the user are two major issues in the protocol design of mobile communications [8-11]. Authenticating mobile users is directly linked to the billings records of wireless mobile communications. When a phone card is used, the card must be authenticated. Card authentication can protect both the cardholders and the HLRs. The verification function can prevent illegal access to cards, which may cause monetary loss to card issuers and cardholders. It is much more easier to authenticate phone cards when the cards are used in the holders' hometowns. For a holder using a card in a visited area, the visited VLR must verify the card before a call can be delivered.

All current mobile communication systems provide certain essential functions of authentication [4, 5, 9, 12]. The designs of authentication protocols rely on the different requirements of the systems. The phone card is appropriate for widespread use under different networks, particularly when a visited area is a foreign domain. This requirement complicates the design of an authentication protocol. Local verification by the visited VLR does not guarantee the legitimacy of a phone card under the circumstances in which the messages are transmitted through different networks. Fig. 3 denotes the basic authentication procedures for a phone card.

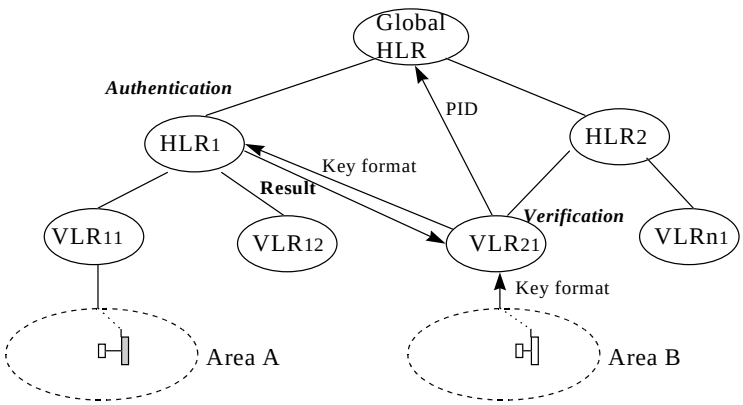

Fig. 3. Authentication process of a phone card.

For an owner using a phone card within the domain where the card is issued, the HLR can easily authenticate the card as each requested call is originated. Because a phone card also provides the service of receiving incoming calls, a cardholder must register his PID using specific telecommunication equipment with the Global HLR. For a user making a call outside of the domestic domain, the visited VLR first reads the key format from the card, obtains the HLR.id of this card, and then passes the user's PID to the Global HLR for

store the location information. According to the HLR.id, the VLR either verifies the key itself or passes the current key to the HLR and awaits the authentication result. The HLR conducts authentication and passes the result (yes/no) to the VLR. The VLR can then verify the legitimacy of the card. If the result is "yes", this the user is allowed to make a call. Otherwise, the VLR rejects the card.

The PID is keyed in by cardholder or read from the card not only to provide the current location of the user, that is, the location of the visited domain and the particular mobile phone, but also to connect the user to the Global HLR. The Global HLR can easily locate the position of this specific mobile phone and identify the user at a distant region.

For commercial applications, various authentication methods can be implemented to deploy a phone card. Therefore, we propose two authentication methods in this study. They are the one-way function approach [13] and the public-key cryptography approach [3].

6.2 Implementation I: One-Way Function Approach

The first proposed authentication approach is the one-way function approach. The key format is designed as follows:

HLR.id	$n, f^{n}(x)$	n-1, $f^{n-1}(x)$	.....	2, $f^{2}(x)$	1, $f(x)$

The Home HLR generates n keys and stores them in each card. The keys are generated by calculating a one-way function $f^{m}(x)$, where $m = n, n$-1, n-2,..., 2, 1. Therefore, the keys are labeled with count numbers in a descending order, i.e., n, n-1, n-2, ..., 2, 1. The Home HLR stores a record of the current number, n, and the current value of the one-way function, $f^{n}(x)$, for each *PID*i. When a cardholder i desires to deliver a call to any place, i.e., either in the home domain or in a visited domain, he/she inserts the card to a mobile phone and keys in his/her PID. Then the data of the HLR.id, the PID, one key and its associated count number are passed to the home HLR through the VLR. Fig. 4 depicts the authentication procedure for using one-way function approach.

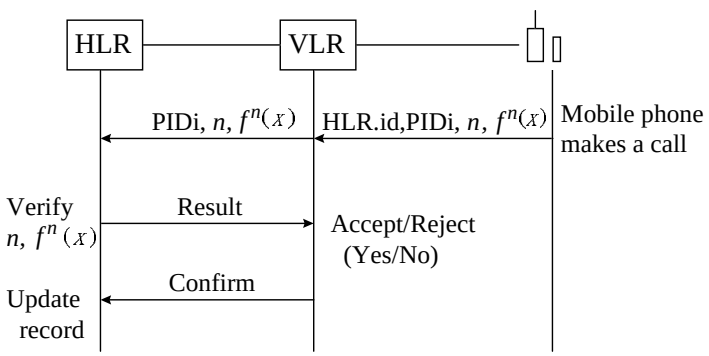

Fig. 4. Phone card authentication using one-way function approach.

The HLR maintains one record for each phone card *i*, i.e., (PIDi, count, key). The initial record for each PIDi is (*null*, n+1, $f^{n+1}(x)$). When a user buys a card, this cardholder can register in the HLR with a freely chosen PIDi for subsequent usage of this card. Thus, the HLR updates the card record by adding the PIDi to it for the first call request. The HLR can verify $f^n(x)$ and n by checking if $f^{n+1}(x) = f(f^n(x))$ and n+1. If they match, the HLR will replace $f^{n+1}(x)$ with $f^n(x)$ and $n + 1$ with n in the card record. The "yes" result is then passed to the VLR, and the request for service can be accepted. In the subsequent jth call origination, the phone card sends the key set $(n - j + 1, f^{n-j+1}(x))$ to the HLR. The HLR verifies the count by adding 1 to it and checks the key to determine whether $f^{n-j+2}(x) = f(f^{n-j+1}(x))$. If they match, the HLR replaces the card record with $(n - j + 1, f^{n-i+1}(x))$ associated this PIDi. Otherwise, the HLR rejects the call request.

6.3 Implementation II: the Public-Key Cryptography Approach

In the one-way function approach, phone card authentication is carried out by the HLR. An alternative means of authentication is carried out by the VLR. This can be implemented by the public-key cryptography approach [3]. The key format for the card is shown as follows:

HLR.id	PIDi	C, $(PIDi)^{d^{2^C}}$	C-1, $(PIDi)^{d^{2^{C-1}}}$	....	2, $(PIDi)^{d^{2^2}}$	1, $(PIDi)^{d^2} \bmod n$

The Home HLR calculates the secret key, d, with the public information, n, which is a product of two primes. The keys are generated from calculating $(PIDi)^{d^{2^m}} \bmod n$, where m = C, C-1, C-2... 2, 1. The *PIDi* assigned by the HLR is the Personal Identity of the cardholder, and m represents the call count. The HLR keeps an initial record (*PIDi*, C) for card i.

When a card is authenticated, the mobile phone transfers one key, its associated Count, and the *PIDi* to the VLR. Firstly, the VLR checks if $[(PIDi)^{d^{2^C}}]^{e^{2^C}} \bmod n = PIDi$ by using the HLR's public key, e, and public information, n. If the calculation is correct, the VLR then transmits the C and *PIDi* to the HLR. Otherwise, the VLR rejects the service request at this moment. Secondly, the VLR waits for the result of verifying C conducted by the HLR. When the "yes" result is received, the VLR can confirm the genuineness of the phone card and provide service. Then, the HLR then updates the C value for this *PIDi*.

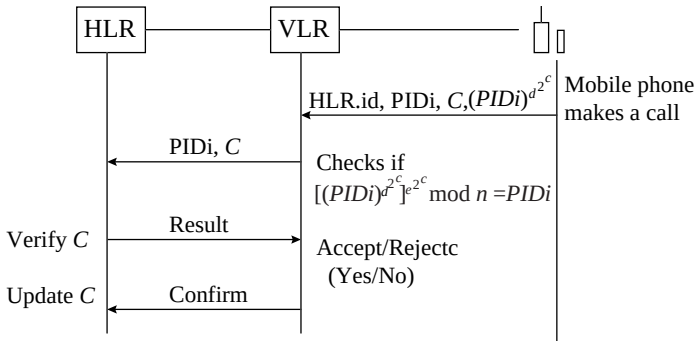

Fig. 5. Phone card authentication using the public-key cryptography approach.

In this method, the public key, *e*, and *n* value of the HLR can be distributed to all the VLRs beforehand. Another alternative occurs when the VLR receives a service request from a *PIDi*; this VLR then requests the HLR to provide *e* and *n*.

6.4 Computational and Capacity Analyses

Both the one-way function approach and public-key cryptography approach maintain only one record instead of requiring storage of key tables for each phone card. Thus, the capacity in the HLR will be a minimum. In this way, the risk of possible leaking of sensitive information can be significantly reduced. Also, these two approaches require only one computation to verify the card, e.g., $f^{n+1}(x) = f(f^n(x))$ in the HLR using the one-way function approach, and $[(PIDi)^{d^{2^c}}]^{e^{2^c}} \bmod n = PIDi$ in the VLR using the public-key cryptography approach.

The security of the public-key cryptography approach rests on the difficulty of factoring the modulus, *n*. This technique has been considered impractical due to the higher computational complexity. Therefore, the computing time is the critical factor for authentication in the public-key cryptography approach. However, in this approach, no computation is needed in the low-cost low-power mobile terminal. The complexity lies in the network equipment; i.e., the only one computation is performed by the VLR. Researches have shown that there are around 210 multiplication for a 512-bit modulus using the Diffie-Hellamn technique [14]. For much better performance in this approach, the VLR's computations can be performed using a special-purpose processor. Examples of such processors are the special-purpose chips described by Brickell in [15], or a Digital Signal Processor (DSP) running an algorithm, such as that described by Dusse and Kaliski in [16]. Dusse and Kaliski claimed performance results that correspond to performing a single 512-bit modular multiplication at around 145 *u*s on a DSP. In this case, 210 modular multiples need only 30 ms. Therefore, a single such processor, acting as an embedded cryptoserver, can perform the public-key computations for 10-20 calls per second, (considering queuing delay), which corresponds to support to 12000-24000 customers (assuming 3 calls per user per hour) [10].

Both implementations need a minimum storage for phone card information and have very acceptable processing time for authentication. It is practical and possible to deploy these two approaches in using the phone card application in the real world.

6.5 Discussion

The *PID* is regarded as a virtual dialing number for a specific cardholder. In the one-way function approach, the *PID* can be freely chosen. When a specific *PID* is keyed in the first time for registration or call request, the HLR will record the *PID* associated with its current phone card. At this moment, the HLR will check the uniqueness of the *PID*. If a duplicate *PID* is chosen by other cardholder, the HLR will ask this cardholder to change it. Though the uniqueness of the *PID* can be maintained within an HLR domain, duplicate *PIDs* can occur among different HLRs. Adding the HLR.id to each *PID* can solve this problem. In the public-key cryptography approach, the *PID* is assigned by the card issuer to represent the user's identity. Since the *PID* is treated as one of the keys, the cardholder cannot choose and change the *PID*. The *PID* will be read automatically from the card when the card is used.

The key replaying problem is a point of concern in implementing authentication methods. Replaying means that VLRs reuse the same keys to charge the HLRs for the unauthorized usage. The VLRs can obtain the keys in the card when the VLRs transmit the keys to the HLR. If the HLR does not perform any check on the used keys, the VLRs can reuse the same key for extra charges. Concerning the key replaying problem, both implementation methods can avoid this by verifying the number of calls, e.g. n in the one-way function approach and C in the public-key cryptography approach, and the computed function value or the computed *PIDi*. A visited VLR cannot reuse or share with other VLRs any used keys from the card.

In the one-way function approach, the HLR maintains the most recent function value, $f^{n-i+2}(x)$, after successfully completing the ith call request authentication. If the VLR reuses the old key, i.e., $f^{n-j+1}(x)$ with the jth call, where $j \leq i - 1$, the HLR will calculate $f(f^{n-j+1}(x)) = f^{n-j+2}(x)$ and find that the value does not matched $f^{n-i+2}(x)$ due to $n - i + 2 \neq n - j + 2$. Attempts to fake a real card can be avoided.

In the public-key cryptography approach, the HLR only maintains the *PIDi* and its correspondent C but not key values. When a VLR verifies the *PIDi* and passes C to the HLR, it also gets this card's current C. The VLR may fabricate a card even though it does not have the keys. The VLR can send HLR the pair of (*PIDi*, C) to update the value of C for this *PIDi* to pretend that it has provided call services. Under these circumstances, two cases can occur. (a) Before the cardholder uses the card again, the VLR uses up all the quota of this card in the HLR's database. Then, the cardholder cannot use this card any more and the VLR will charge the HLR more. (b) When the card holder uses the card in a subsequent call request, the new VLR rejects the request due to the unmatched C. To avoid monetary loss for both the HLR and card holder, the HLR must be capable of tracing the false billing from the untrusted VLRs. A possible way to solve the replaying problem in the public-key cryptography approach is to decode the key format and check the quota remaining in the phone card when the card holder finds a replaying or fabrication problem. Also, some feasible refund methods should be provided for customers in both cases of replaying problems.

7. OPERATIONAL CONSIDERATIONS AND CONCLUSIONS

The phone card provides a valuable alternative to the SIM card in wireless mobile communications. Realizing the phone card application and authentication requires that the following problems be solved.

(1) With respect to commercial design of a mobile handset, dual use of a phone card and SIM can be built into a handset with switchable modes. Each mode can perform its own specific authentication. This dual mode can also use the software design to distinguish between the inputs of a SIM from that of a phone card.
(2) Importantly, the methods proposed herein serve as vehicles for authenticating phone cards within a network or even among different networks, regardless of the individual system's specific method of authentication. If a separate authentication process is maintained for each independent system [4, 12] without application of the new integrated

approaches to the protocol design, using the phone card will inevitably be used just like the SIM. Under these circumstances, the advantage of applying one more alternative to mobile communications will disappear.

The phone card can be a value-added alternative to the SIM and an effective means of expanding the market of mobile communications. Solutions to location tracking, authentication, and billing scheme problems make the versatile use of the mobile phones possible. The phone card retains the merits of the SIM card, and eliminates the constraints that exist in the SIM card. Even if a phone card is lost, the financial risk will be much less than that of losing a SIM card. The ideas and technical approaches of the phone card application presented in this article provide more channels for mobile communications and enhance the technology of mobile telecommunications.

REFERENCES

1. T. Grigorova and I. Leung, "SIM cards," *Telecommunication Journal of Australia*, Vol. 43, No. 2, 1993, pp. 33-38.
2. R. Hagen, "Security requirements and their realization in mobile networks," *The Fourteenth International Switching Symposium '92*, Vol. 1, 1992, pp. 127-131.
3. R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signature and public-key cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 120-126.
4. EIA/TIA, "Cellular radio telecommunications intersystem operations: authentication, signaling message encryption, and voice privacy," Technical Report, TSB-51, Electronic Industries Association/Telecommunication & Industry Association, 1993.
5. E. Lycksell, "GSM system overview," Technical Report, Swedish Telecommunication Admin., 1991.
6. M. Mouly and M. B. Pautet, *The GSM System for Mobile Communications*, M. Mouly, 49 rue Louise Bruneau, Palaiseau, France, 1992.
7. J. E. Wilkes, "Privacy and authentication needs of PCS," *IEEE Personal Communication*, Vol. 12, No. 4, 1995, pp. 11-15.
8. A. Aziz and W. Diffie, "Privacy and authentication for wireless local area network," *IEEE Personal Communication*, Vol. 1, No. 1, 1994, pp. 25-31.
9. J. Beheim, "Security first in Europe's mobile communication," *Telecommunication Report International*, Vol. 17, No. 1, 1994, pp. 31-34.
10. M. J. Beller, L. F. Chang and Y. Yacobi, "Privacy and authentication on a portable communications system," *IEEE Journal on Selected Areas in Communication*, Vol. 11, No. 6, 1993, pp. 821-829.
11. E. Zuk, "GSM security features," *Telecommunication Journal of Australia*, Vol. 43, No. 2, 1993, pp. 26-31.
12. European Telecommunications Standards Institute, "Security related network functions," Technical Report, Recommendation GSM 03.20, 1993.
13. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc., 1994.
14. Y. Yacobi, "Discrete Log with compressible exponents," *Advances in Cryptology-*

CRYPTO '90, Santa Barbara, CA, Aug. 1990, pp. 639-643.
15. E. F. Brickell, "A survey of hardware implementations of RSA," *Advances in Cryptology-CRYPTO '89*, Santa Barbara, CA, 1989, pp. 20-24.
16. S. R. Dusse and B. S. Kaliski, "A cryptographic library for the motorola DSP56000," in *Advances in Cryptology-Eurocrypt '90*, Lecture Notes in Computer Science, I.B. Damgard, Ed. New York: Springer-Verlag, 1991, pp. 230-244.

Chii-Hwa Lee received the BS degree from National Taiwan University, Taiwan, in 1976, the Master of Computer Science from Texas A&M University, USA, in 1982, and the Ph.D. degree in computer and information science in National Chiao Tung University, Taiwan, in 1998. She joined the projects of the C3I System in the Chung Shang Instituite of Science and Technology (CSIST) under the Department of Defense, Republic of China, in 1985. She was also the Head of the Management Information System of CSIST from 1988 to 1993. Her current work is related to the secure databases for intelligent systems. Her research interests include data security, mobile communications, mobile computing, and database systems.

Min-Shiang Hwang received the BS degree in EE from the National Taipei Institute of Technology, Taiwan, in 1980; the MS degree in EE from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan, in 1995. He was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications. He was also a project leader for research in computer security at TL since 1990. He has been on the faculty of the Department of Information Management at Chao Yang University of Technology, Taiwan, since 1996. He is a member of IEEE and ACM. His research interests include cryptography, data security, database systems, and network management.

Wei-Pang Yang was born on May 17, 1950, in Hualien, Taiwan, Republic of China. He received a B. S. degree in mathematics from National Taiwan Normal University in 1974, and an M. S. and a Ph.D. degree from National Chiao Tung University (NCTU) in 1979 and 1984, respectively, both in computer engineering.

Since August 1979, he has been on the faculty of the Department of Computer Engineering at NCTU, Hsinchu, Taiwan. In the academic year 1985-1986, he was awarded the National Postdoctoral Research Fellowship and was a visiting scholar at Harvard University. From 1986 to 1987, he was the Director of

the Computer Center of NCTU. In August 1988, he joined the Department of Computer and Information Science at NCTU and acted as the Head of the Department for one year. Then he went to the IBM Almaden Research Center in San Jose, California for another year as a visiting scientist. From 1990 to 1992, he was the Head of the Department of Computer and Information Science again. His research interests include database theory, database security, object-oriented database, image database, and Chinese database systems.

Dr. Yang is a member of IEEE, ACM, and the Phi Tau Phi Society. He was the winner of the 1988 and 1992 Acer Long Term Award for Outstanding M. S. Thesis Supervision, and the winner of 1990 Outstanding Paper Award of the Computer Society of the Republic of China. He also obtained the 1991-1993 Outstanding Research Award of the National Science Council of the Republic of China.