http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 7 (2): 261-268, 2008
ISSN 1812-5638

A Secured Mobile Access Scheme for SMS Message

[1]Rongyu He, [1]Zheng Qin and [2]Xi Qin
[1]School of Electronic and Information Engineering, Xi'an Jiaotong University,
Xi'an, 710049, People's Republic of China
[2]School of Electronic Technology, Information Engineering University,
Zhengzhou, 450004, People's Republic of China

Abstract: In this contribution, we firstly design and realize a PKI-SIM card that is a regular SIM card with additional PKI-functionality and present a security mobile access scheme based on the PKI-SIM card, which offers solutions for the development of secure mobile business applications using SMS. Then, we proposed a novel authentication and session key distribution protocol which provides end-to-end confidentiality and integrity of the SMS message. Finally, a formal verification of the protocol using BAN logic is presented and the security and performance analysis of our scheme revealed that it is suitable for practical needs both in speed and security

Key words: PKI-SIM card, session key, primary key, PLMN, strong authentication

INTRODUCTION

Since the first SMS (Short Message Services) message was sent in the UK in 1992, the SMS has become a mass communication tool. The mobility, ubiquity and low cost of SMS make it become a very attractive bearer for mobile applications. But when SMS becomes a bearer for commercial or governmental applications, such as electronic bank, the security and trust concerns emerge.

The SMS was primarily developed to allow short text messages (up to 160 characters) to be exchanged between mobile devices as well as between a mobile device and a data-centric application such as Mail2SMS (an E-mail arrive notice application). It is a store-and-forward service and inherently is in plaintext. Although the Public Land Mobile Network (PLMN) traffic, such as GSM, is usually encrypted, it provides no protection for the SMS messages when it is zipping around the core network or waiting in a queue at the Short Message Service Center (SMSC), or when it is sitting in the memory of the handset (Guthery and Cronin, 2002). For transmitting confidential data or providing private service by SMS over the PLMN, a reasonable level of security must be guaranteed for the authentication and privacy.

The authentication and privacy are two basic requirements for mobile applications security. Authentication prevents unauthorized and forgery in network services, while privacy protects sensitive data against eavesdropping and modification (Shieh *et al*., 1999). The European Telecommunications Standards Institute (ETSI) introduces the TS 03.48 specification (3GPP, 2005) that provides end to end security services for an SMS message going to or coming from the SIM card. However this specification is limited to the use of secret key techniques for message privacy and doesn't support public key techniques for the message authentication.

In order to protect the remote resources, numerous remote authentication schemes are proposed. Among them, password-based remote authentication is one of the most commonly used authentication techniques because of its simplicity and effectiveness. But it is both weak and not user-friendly due to its plurality. For services such as e-commerce, online banking, government portal, corporate Intranet access, etc., strong authentications are required. Due to the capable of storing and computing essential information with properties such as tamper-resistance, smart cards have been widely adopted in strong authentication schemes. The SIM (Subscriber Identity Module) card used in mobile phone is the most popular smart card and it would be very convenient and cost-efficient when SIM card is applied into the authentication schemes.

The literature (Wangensteen *et al*., 2006) proposed a generic authentication system for Internet services using the regular SIM card and the system provides a strong authentication mechanism for a fixed Internet computer based upon the GSM authentication infrastructure.

Corresponding Author: Rongyu He, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, 710049, People's Republic of China

Similarly, the literature (Torres *et al*., 2007) mainly discussed ways of using smart card for application authentication over the wired network. However, the properties of the wireless network are different from that of the wired network and the authentication and communication schemes used in the wired network can not be applied into the wireless network directly.

Recently, some authentication schemes using smartcard or SIM card over mobile network are proposed. The system in (Hassinen and Hypponen, 2005) uses the asymmetric algorithm (RSA) for protecting SMS message. But the digital signature and decryption operator, which all are computation-intensive public key operators, are performed by SIM card and these make the system has a long delay for each message exchange. The system in (Chanson and Cheung, 2001) needs a trusted third party server in the Internet and requires the mobile user place his/her full trust in the remote network entity. This means that the system is vulnerable if the trusted third party is compromised. Moreover, the fact of using dual slot mobile phone prevents its pervasion. The scheme in (Jordi and Josep, 2003) uses mobile device and wireless personal area networks, like Bluetooth, instead of smart cards to store private information and performs cryptographic operations, in this case the secret keys stored in the memory of the mobile device exposes security issues such as the keys could be infected by viruses or be maliciously replaced. Authors of (Lee *et al*., 2006; Juul and Jorgensen, 2002) didn't mention how to apply the wireless PKI architecture to provide end-to-end security between the mobile phone and the service provider. Literatures (Hsu, 2004; Chien *et al*., 2002; Juang, 2004; Lee *et al*., 2005; Liaw *et al*., 2006) proposed the password-based remote user authentication schemes using smart card without maintaining the password table, but they do not provide the session key negotiation and distribution mechanism over the PLMN. In addition, the schemes in (Hsu, 2004; Chien *et al*., 2002; Juang, 2004; Liaw *et al*., 2006) have not considered the protection mechanism in their protocols to prevent the offline dictionary attack with the smart card.

PKI-SIM CARD AND SECURE MOBILE ACCESS SCHEME

The design of PKI-SIM card: As a tamper-resistant device, the SIM card in the mobile phone is most widely used due to the high penetration of mobile phones and it has been widely adopted in remote authentication schemes because of the low cost, the portability and the cryptographic capacity. Moreover, the standardization of the SIM Application Toolkit with the advancement in the hardware platform for the SIM created an ever advancing platform for secure data services at the discretion and under the control of the operator and the service provider. The PKI-SIM is a regular SIM card with additional PKI-functionality, as Fig. 1 shown. It is used to store the secret keys and the user's credentials and perform cryptographic operations on the chip without exposing these secret keys.

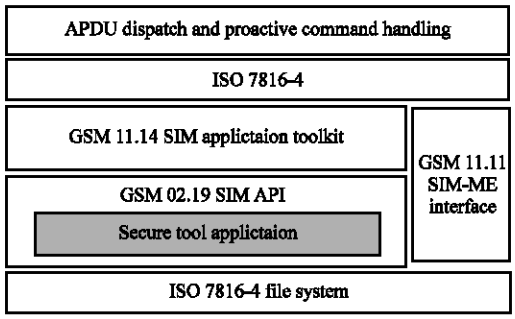

Fig. 1: Architecture of a PKI-SIM card

The PKI-SIM is encapsulated accommodating to ISO 7816-4 specifications and conforms to all SIM card standards and specifications. It can be used in any mobile phone which support STK function and has the same communication functionality as well as regular SIM card.

In the PKI-SIM, an additional module, named Security Tool Application (STA), provides cryptography functionality for the SIM Toolkit (STK) applications. The STA is implemented in assembler running on the cryptographic co-processor on-board the PKI-SIM and provides cryptographic primitives including hash functions, asymmetric cryptographic function and symmetric cryptographic functions. The STK application can invoke these cryptographic functions according to SIM API (GSM 02.19). Furthermore, the STA module makes the secure protocol (which is mentioned in section III) steps as transparent as possible to the STK applications.

The general protocol of communication between SIM and mobile phone is described in ISO7816-4. The secure SMS message sent from SAG is class 2 message. When the mobile device received the secure SMS message, it passes the messages to PKI-SIM card directly. The mobile phone utilizes the APDU commands, according to the standardized T = 0 protocol, to move data from the ME to the PKI-SIM card.

The secure remote access scheme: Using the PKI-SIM card as tampered resistant device, we proposed a secure mobile access scheme with strong authentication using

SMS as bearer. The secure scheme consists of client devices (mobile device with PKI-SIM), a Certification Authority (CA), Secure Access Gateway (SAG) and Mobile Operator. The overview of the scheme is shown as Fig. 2.

The CA conducts unified administration of public key and publicize public key in form of public key certification and maintains a directory database (LDAP) containing the certificates of users and a Certificate Revocation Lists (CRLs). The CA can be either a governmentally controlled CA for general purpose, or a PKI technology based server for specific purpose.

In our security scheme the PKI-SIM card acts as a tampered resistant device and a cryptographic device for the mobile device. It stores the secret keys and the user's credentials and performs cryptographic operations on the chip without exposing these secret keys. Furthermore, any STK application can be downloaded on PKI-SIM card via Over the Air (OTA).

The SAG, which is a SMS gateway with security functionalities, is residing in service providers' infrastructure and is operated by the service provider. It communicates with the SMSC (Short Message Service Center) via SMPP protocol over TCP/IP and takes the responsibility for receiving/sending SMS messages from SMSC, authenticating the mobile user and establishing a secure connection between the SAG and PKI-SIM card. A PKI-based separated computing device is used to store private keys and perform the cryptographic operations without exposing them. The separated computing device is a high performance PCI interface-based peripheral that contains the processor, algorithms and cryptographic material. It is co-operated with PKI-SIM to ensure security at the application level, includes authentication, confidentiality, integrity and non-repudiation.

The Mobile Operator provides the communication infrastructure and its main duty is to route the SMS messages to the destination. The Mobile Operator is unable to read the SMS message contents since they are encrypted at the source.

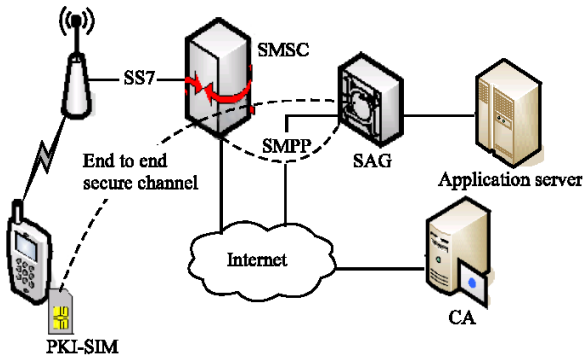

Fig. 2: The overview of the secure scheme

PROTOCOL FOR SECURE SHORT MESSAGE EXCHANGE

The secure SMS message structure: The SMS message is comprised of two portions, the SMS header and the payload. The SMS header includes destination address, originating address, at least 5-byte metadata and the size of the user data field. The payload is the user date field, which is the content of the message and its maximum length is 160 characters.

Because the secure SMS message is forwarded to the PKI-SIM card and processed by the STK routine when it is received at the mobile phone, some secure parameters must be contained in the SMS message, which tells to the PKI-SIM card what the purpose of the SMS message is and how the user data is secured. The secure parameters occupy the user data field in our scheme. Therefore, the payload of secure SMS message is composed of two parts: a command header and the encrypted user data. The command header occupies the first 12-bytes of the valid capacity of the short message. The details of the command header are shown in Table 1 and the purpose of each data field of the secure header is briefly examined as follow:

Flag: Security indicator and the service provider identificator. The first bit of the field is used to identify whether it is a secure SMS message. If the first bit is 1, it represents that the SMS message is a secure SMS message and the last 7 bits are used to store the codename of a service provider that indicates which SAT application should handle the secured data.

App style: This field is 1 byte long and consists of 3 bits giving the protocol version and 5 bits of the short message style, it is shown in Fig. 3. Both the sender and receiver must have the same version number. They deal with the secure SMS message in a same way. In our protocol, there are seven different messages used for authentication, primary key negotiation, data communication and some status report. The SMS style indicates which style the SMS message is and the SAT application how to respond to this message.

Table 1: The SMS message data fields

Field name	Bytes	Description
Flag	1	Identifies the service provider
App style	1	Identifies the version number and SAT style
Algorithm	1	Reference to the algorithm used to compute the encrypted payload
CNT	1	Replay detection and sequence integrity counter
DF	4	Diversification factor
MAC	4	Message authentication codes
Encrypt DATA	128	Effective payload

Protocol version	Message style
	00000: Send from PK-SIM, request primary key agreement
	00001: Send from PK-SIM, acknoeledge the new primary key primary
	00010: Send from PK-SIM, encrypted SMS
	00011: Send from PK-SIM, alert report
	10001: Send from SAG, a response from primary key agreement request
	10010: Send from SAG, a encrypted SMS
	10011: Send from SAG, alert report
	Other are researved for further extension

Fig. 3: Fields of the app style

Algorithm: Identifies which cryptographic algorithm is used for data encryption in the secure SMS message. Because of the limited storage capacity, there are only three symmetric cryptographic algorithms are integrated into the PKI-SIM card. They are two general algorithms such as 3DES and AES and a dedicated algorithm for specific purpose.

CNT: This field indexes all the messages between the SAG and the PKI-SIM card. Its extended purpose is to counter a replay attack. The length of this field is 1 byte. Before sending the SMS message, both sides will first add 1 to the counter. If the index value received is larger than local one but falls within a certain predefined range, this message will be accepted. Otherwise, it will be rejected.

DF: A 4-byte long diversification factor, which is used to generate a session key derived from primary key. The communication initiator, either PKI-SIM card or SAG, randomly generates the diversification factor as a plaintext. After getting the encrypted SMS message, the receiver will take use of the received diversification factor to diversify the primary key generated in authentication phase and then the same session key will be generated.

MAC: It is a 4-byte Message Authentication Code used to ensure data integrity. It is the first 4-byte of the hashing value of message, DF||primary key||Message.

Encrypted data: The actual payload, which is encrypted by the algorithm indicated in Algorithm field. A valid message payload is up to 128 characters.

In our protocol, the first twelve bytes of a SMS message are used for secure parameters, therefore, there is only 128 bytes of a SMS are used for the valid payload and the efficiency ratio is 91.4%.

Protocol for secure short message exchange: Using PKI-SIM, we propose a PKI-based authentication and session key distribution protocol for the SMS. Our protocol consists of three phases: Registration phase, Authentication phase and Session phase. The detail is described as following:

The registration phase: The registration phase makes the PKI-SIM apply for a certificate from the CA and complete the pre-register to a service provider by download the certificate of the SAG of the service provider.

Step 1: The PKI-SIM generates a pair of keys, one private key named SKME and one public key named PKME, according to secure requires and uploads the public key to the CA where the certificate of the PKI-SIM card is generated.

Step 2: The PKI-SIM downloads the SAG's public key from the CA and stores it as root public key on the chip.

Step 3: The PKI-SIM is issued to a user.

The authentication phase: In the authentication phase, the PKI-SIM and the SAG mutually authenticate each other by the certificate and negotiates a primary key shared between them. Before the authentication phase, the user must become a registered user of the SAG, this is an enrollment process specified by service provider and not in scope for this study. The authentication phase is illustrated in the following diagram as shown in Fig. 4.

Step 4: PKI-SIM → SAG: ID_{ME}, N_C, Seq

Step 5: SAG → PKI-SIM: $\{N_S, UAKey\}PK_{ME}$, $\{H(N_S, N_C, ID_{ME}, UAKey)\}SK_{SAG}$

Step 6: PKI-SIM → SAG: N_S

In step 4, the PKI-SIM sends two random numbers, N_C and Seq and its identifier, ID_{ME}, to the SAG.

In step 5 the SAG firstly checks the validity of the mobile user, ID_{ME}, according to registration information. If it successes, the SAG fetches the PKI-SIM's certificate from the CA or PKI server according to the ID_{ME}, then it randomly generates N_S and calculates UAKey (the primary key) from f ($N_C||N_S$). Finally, it encrypts these numbers with the public key, PKME, of the PKI-SIM and sends it to PKI-SIM with his digit signature $\{H(N_S, N_C, ID_{ME}, UAKey)\}$ SK_{SAG}.

On receiving the message from the SAG in step 6, the PKI-SIM decrypts it and verifies the digit signature. If the verification is success, it accepts UAKey as primary key and sends the random number, N_S, back to informing SAG that the primary key is accepted. In this time, the primary key UAKey between the PKI-SIM card and SAG is established.

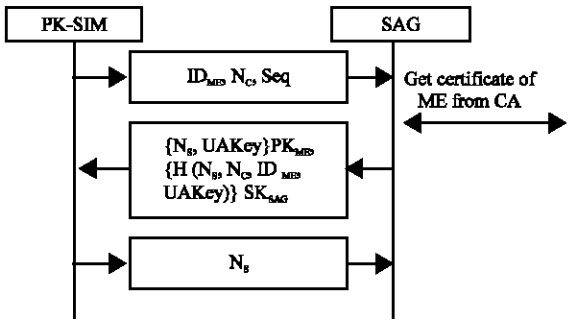

Fig. 4: The authentication phase

The session phase: The session phase allows the PKI-SIM or the SAG to create a one-time pad session key used for protecting the privacy of the SMS message during a session. When the user wants to send a secure SMS message, M, to the SAG in valid period of the UAKey, he can initiate the session phase by generating a session Key based on the primary key UAKey.

The PKI-SIM randomly generates a 4-byte random number Na as the Diversification Factor (DF) and calculates a session key (sK) by diversifying the UAKey with the Na, then it encrypts message M by the session key (sK). In order to prevent tampering and counterfeiting, a 4-byte Message Authentication Code (MAC) which is the first four bytes of the hash value of message, Na||UAKey||M, is sent along with the Na and other secure parameters mentioned in section III.A. The main fields of the secure SMS, Secure-M, are described as follow:

$$\text{Secure-M} = \{Na, ID_{ME}, MAC)\}, E_{sK}(M)$$

where, MAC is the first four bytes of H(Na||M||UAKey).

When receiving the Secure-M, the SAG derives the ID_{ME} and Na from the secure SMS message, fetches the ME's UAKey, which is stored in SAG according to ID_{ME} and regenerates the Session Key by diversifying UAKey with Na. The SAG uses the session key to decrypt $\{M\}E_{sK}$, get the plaintext M, then it recalculates the MAC with its UAKey and compares the new MAC with the MAC coming from the PKI-SIM. Both MACs will match if the message has not been tampered with. Otherwise, the SAG will discard the receive datum and return a message to notice the PKI-SIM an error occurs.

The process of the SAG sending secure SMS message to a PKI-SIM is similar with that of a PKI-SIM sending secure SMS message to the SAG.

The authentication phase is the most time-consuming part of the protocol, so the primary key will be kept for a period of time in order to reduce PKI based calculation in PKI-SIM card. The maximum value of validity period of a primary key is specified by the user. A session key derived from the primary key is valid during a transaction and a new session key is derived for the next transaction.

ANALYZES THE SECURITY OF OUR PROTOCOL

Authentication proof based on BAN logic: The main goal of our authentication protocol is that the mobile user C and service provider S are believed there is a primary key shared secretly between them. We demonstrate the authentication protocol by BAN logic (Burrows *et al*., 1990; Syverson and Cervesato, 2001). The constructs of the BAN logic as follows:

$P \mid\equiv X$: P believes X, or P would be entitled to believe X.
$P \triangleleft X$: P sees X. Someone has sent a message containing X to P.
$P \mid\sim X$: P once said X. The principal P at some time sent a message including the statement X.
$P \Rightarrow X$: P has jurisdiction over X.
$\#(X)$: The formula X is fresh.
$P \overset{K}{\longleftrightarrow} Q$: P and Q may use the shared key K to communication.
$\overset{K}{\longrightarrow} P$: P has K as a public key. The matching secret key denoted K^{-1}.
$P \longrightarrow Q$: {mesage}: This denotes that the principal P sends the message and that the principal Q receives it.

To analyze our proposed protocol in simplification, we first give some assumptions as follows:

P1: $C \mid\equiv \overset{K_c}{\longrightarrow} C$
P2: $C \mid\equiv \overset{K_s}{\longrightarrow} S$
P3: $C \mid\equiv \#N_c$
P4: $C \mid\equiv S \Rightarrow C \overset{K_{cs}}{\longleftrightarrow} S$
P5: $S \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S$

Then we transform our protocol into the idealized form as follows:

Step 7: $C \rightarrow S: N_c$ .....from..C

Step 8: $S \rightarrow C: \left\{ \left\{ C \overset{K_{cs}}{\longleftrightarrow} S, N_c, N_s \right\}_{K_s^{-1}} \right\}_{K_c}$ .....from.S

Step 9: $C \rightarrow S: N_s$.....from..C

The main steps of the proof are shown in the following:

By step 8, we apply the annotation rules (Burrows *et al*., 1990) to yield that:

$$C \lhd \left\{ \left\{ C \xleftrightarrow{K_{cs}} S, N_c, N_s \right\}_{K_s^{-1}} \right\}_{K_c} \quad (1)$$

By formula 1 and assumption P1, the message-meaning rule for public keys (Burrows *et al*., 1990) applies and yields the following:

$$C \lhd \left\{ C \xleftrightarrow{K_{cs}} S, N_c, N_s \right\}_{K_s^{-1}} \quad (2)$$

Similarly, by formula 2 and assumption P2, we derive:

$$C \mid\equiv S \mid\sim \left\{ C \xleftrightarrow{K_{cs}} S, N_c, N_s \right\} \quad (3)$$

From assumption P3, we get:

$$C \mid\equiv \#\left\{ C \xleftrightarrow{K_{cs}} S, N_C, N_S \right\} \quad (4)$$

By formulas 2 and 4, the nonce-verification rule (Burrows *et al*., 1990) applies and yields:

$$C \mid\equiv S \mid\equiv \left\{ C \xleftrightarrow{K_{cs}} S, N_C, N_S \right\} \quad (5)$$

By formula 5, we break a conjunction, to obtain the following:

$$C \mid\equiv S \mid\equiv C \xleftrightarrow{K_{cs}} S \quad (a)$$

By (a) and assumption P4, the jurisdiction rule (Burrows *et al*., 1990) applies and yields the following:

$$C \mid\equiv C \xleftrightarrow{K_{cs}} S \quad (b)$$

By step 9, the annotation rules (Syverson and Cervesato, 2001) apply and yield that:

$$S \lhd N_s \quad (6)$$

By assumption P5, we know:

$$S \mid\equiv C \xleftrightarrow{K_{cs}} S \quad (c)$$

For only C can get by decrypt the message 2 with his private key, so we have

$$S \mid\equiv C \mid\equiv C \xleftrightarrow{K_{cs}} S \quad (d)$$

According to the above, the first order belief (b) and (c) and the second order belief (a) and (d) are obtained. It is proved by BAN logic that the protocol is security.

Security analysis: The security of our scheme is examined as follows:

- All the secret keys used in our scheme are privacy. In the mobile terminal, the PKI-SIM is used as storage and cryptographic device. All the cryptographic operations are performed in this cryptographic device and all the secret keys such as private key and primary key are stored in this tamper-resistant device and never exposed to any third party. In the SAG, a separate computing device, similar as PKI-SIM in mobile phone, is used as cryptographic device and the primary keys are stored in its encrypted form when they are out of the cryptographic device and are recovered to its original form only when it is read in cryptographic device to perform cryptographic operations. This means that only the cryptographic devices know the secret keys, i.e., the secret keys are not exposed out of cryptographic device.
- The replay attack is prevented because the freshness of the messages can be verified through the Nonce. In the authentication phase, the random number, Seq and Ns, are used as a Nonce, respectively; in the session phase, a side effect of the diversification factor Na is used as a Nonce.
- Even if the session key is compromised, the known key attack still fails because the attacker also has to know the primary key, UAKey, to compute the new session key. The attacker can not get the primary key, UAKey, from the client side because it is stored in the read-protected area of the PKI-SIM and only the legal user who knows the PIN can active the cipher functionalities of the PKI-SIM card to compute the new session key sK = f(UAKey,Na). The attacker either can not get the primary key, UAKey, from the SAG side because all the primary keys stored in SAG are encrypted with a protect key.
- If an illegal user tries to request the authentication, he has to know the private key of the legal user. However, the private key of the legal user is stored in the tamper-proof secured file structure of the user's PKI-SIM and never be exposed to any third party -- that means no adversary can spy the key. So it is

infeasible because it has no way to get the private key to decrypt the message in step 5. If a masqueraded server tries to cheat the requesting user, it has to sign the message in step 5. However, it is infeasible because the masqueraded server has no way to know the private key of the SAG and can't compute the valid digital signature, due to the fact that the private key of the SAG never be exposed.

- The scheme can also defense against the Man-in-the-Middle attack. An attacker intercepts the message in step 4, he replace ID_{ME} with his identifier, $ID_{ME'}$, then sends the modified message to SAG. When received the responded message form SAG, he decrypt the $\{NS\ UAKey\}PK_{ME'}$ with his private key and re-encrypted it with the PK_{ME}, then sends the tampered responded message to original PKI-SIM. Thereby, the attacker knows the primary key. Notice, however, that in this case there will be a mismatch between the signature and encrypted message in step 5 because the SAG's signature includes the identifier, $ID_{ME'}$, of the attacker. It is impossible for an attacker to divert a legitimate signature to another user.

The performance evaluation of the scheme: The PKI-SIM we designed is capable of finish 1024-bit RSA signature generation and verification 4 times and 56 times per sec, respectively and running the SHA-1 (160-bit) hashing operation 1320 times per sec. It embeds a dedicated symmetric cryptographic algorithm (128-bit) approved by OSCCA and can run this cryptographic operations more than 125 times per sec on the card. The PLMN is the GSM cellular network of the China Mobile Communications Corp.

To test the overhead a user would see in using a mobile phone with PKI-SIM, he performs the primary key rekeying operation 20 times. This operation triggers the authentication phase of our protocol where a new primary key establishment. The second column of Table 2 shows the delay in sec, averaged across all 20 runs. It requires approximate 16 sec to authenticate each other and establish a new primary key.

We send SMS message to a SAG 30 times by a mobile phone with a SIM and a PKI-SIM, respectively. The time of the message arriving SAG with SIM and with PKI-SIM are showed in the 3rd and 4th columns of Table 2. The average delay time of the encrypted SMS transmission is approximately 2 sec, which is acceptable for SMS message transmission.

The authentication phase needs to perform the computation intensive public-key operation online and this is the most time-consuming operation. Fortunately, it only needs to be done once in a reasonable period and it is acceptable for security. The session phase only needs hash operation and symmetric cryptographical operations which are computationally cheap, but the session key is a one-time pad key which guarantees the high confidentiality for the communicating parties.

Table 2: Delay of time (sec)

	Establishment time delay	Session time delay	
		SIM	PKI-SIM
Max	19.0	6.0	7.0
Average	15.7	3.0	5.2
Min	9.8	2.3	4.2

CONCLUSIONS

We design and realize a PKI-SIM card which provides a tamper-resistant storage and an execution environment for security critical data and operations. The PKI-SIM card is regular SIM card with additional PKI functionality and cryptographical functionality. It can be used in any regular mobile phones which support STK function and has the same communication functionality as the ordinary SIM card.

We have also proposed a protocol for secure SMS message transmitting that provides strong authentication of communicating parties, effective non-repudiation and full confidentiality of the messages. And a formal proof is given using BAN logic which proves that the protocol is a secure mutual identification scheme.

The performance evaluation shows that there is only 2 sec delay for sending a SMS message to SAG or receiving a SMS message from SAG using PKI-SIM than that use ordinary SIM card. The results demonstrate that the PKI-SIM is suitable for actual needs both in speed and security.

ACKNOWLEDGMENTS

The authors wish to thank Beijing Watchdata Systems Co., Ltd. for the implement of the PKI-SIM card. Our work was supported in part by the National Grand Fundamental Research 973 Program of China (No.2004CB719401).

REFERENCES

3GPP, 2005. Security mechanisms for the SIM application toolkit v.8.9.0, TS 03.48, 3GPP.

Burrows, M., M. Abadi and R. Needham, 1990. A logic of authentication. ACM. Trans. Comput. Syst., 8 (1): 18-36.

Chanson, S. and T. Cheung, 2001. Design and implementation of a PKI-based end-to-end secure infrastructure for mobile E-Commerce. World Wide Web J., 4 (4): 235-253.

Chien, H.Y., J.K. Jan and Y.M. Tseng, 2002. An efficient and practical solution to remote authentication: Smart Card. Comput. Sec., 21 (4): 372-375.

Guthery, S.B. and M.J. Cronin, 2002. Mobile Application Development with SMS and the SIM Toolkit. McGraw-Hill Companies, Inc.

Hassinen, M. and K. Hypponen, 2005. Strong mobile authentication. 2nd International Symposium on Wireless Communication Systems, pp: 96-100.

Hsu, C.L., 2004. Security of Chien *et al.*'s remote user authentication scheme using smart cards. Comput. Standards and Interfaces, 26: 167-169.

Jordi, H.J. and P.B. Josep, 2003. A personal authentication scheme using mobile technology. In: Proceedings of the International Conference on Information Technology: Computers and Communications (ITCC.03).

Juang, W.S., 2004. Efficient password authenticated key agreement using smart cards. Comput. Secur., 23 (2): 167-173.

Juul, N.C. and N.H. Jorgensen, 2002. Security issues in mobile commerce using WAP. Proceedings of the 15th Bled Conference in Electronic Commerce-e-Reality: Constructing the e-Economy, pp: 444-462.

Lee, S.W., H.S. Kim and K.Y. Yoo, 2005. Improvement of Chien *et al.*'s remote user authentication scheme using smart cards. Computer Standards and Interfaces, 27: 181-183.

Lee, C.S. *et al.*, 2006. Design of user authentication system based on WPKI. Proceedings of the 10th International Conference on CSCW in Design, pp: 979-983.

Liaw, H.T., J.F. Lin and W.C. Wu, 2006. An efficient and complete remote user authentication scheme using smart cards. Math. Comput. Model., 44 (1-2): 223-228.

Shieh, S.P., F.S. Ho and Y.L. Huang, 1999. An efficient authentication protocol for mobile networks. J. Inform. Sci. Eng., pp: 505-520.

Syverson P. and I. Cervesato, 2001. The Logic of Authentication Protocols, in LNCS. Vol. 2171, Springer-Verlag, pp: 63-136.

Torres, J., A. Izquierdo and J.M Sierra, 2007. Advances in network smart cards authentication. Comput. Networks, 51 (9): 2249-2261.

Wangensteen, A., L. Lunde, I. Jorstad and T.D. Van, 2006. A generic authentication system based on SIM. International Conference on Internet Surveillance and Protection, Cap Esterel, French Riviera.