GSM Mobile SMS/MMS using Public Key Infrastructure: m-PKI

NOR BADRUL ANUAR, LAI NGAN KUEN, OMAR ZAKARIA, ABDULLAH GANI, AINUDDIN WAHID ABDUL WAHAB
Department of System & Computer Technology
Faculty of Computer Science and Information Technology
University of Malaya
50603 Kuala Lumpur
MALAYSIA.
badrul@um.edu.my, laingankuen@yahoo.com, omarzakaria@um.edu.my, abdullah@um.edu.my, ainuddin@um.edu.my

Abstract: Presently, mobile handheld device has successfully replaced traditional telephone to become the most popular wireless communication tools. Mobile Short Message Service (SMS) and Multimedia Message Service (MMS) fulfill almost all the user requirements as an effective communication and information delivering service. Since SMS/MMS become so popular on daily communication, there is a demand to communicate or exchange confidential information in a secure environment. Public Key Infrastructure (PKI) is a proven solution, which using pairing of key, for secure communication encryption. In this paper, m–PKI is introduced to provide PKI encryption to the mobile SMS and MMS. This new approach allows the end-user to send private and classified message via SMS. The key pair generation and distribution are performed by the Certificate Authority (CA). The size of the key pair are studied and decided by the tradeoff between performance and security.

Key-Words: cryptography, message classification, PKI, SMS/MMS, RSA

1 Introduction

Short Message Service (SMS) has changed the way people communicate. The latest mobile data services report which conducted by Mobile Data Association (MDA) showed that the SMS usage is emerging. According to the statistic [1], UK mobile users had sent out six billion text messages in December 2007 which is almost five thousands SMS per second. The total volume of SMS also increase from 42 billion (2006) to 57 billion (2007). Apparently, society has become so dependent on SMS that the lack of it would be a major disruption.

Recently, a survey carried by IDC shows that more 90% of mobile users prefer SMS as their main communication tool. This survey included 4,056 urban mobile users in Australia, Hong Kong, Malaysia, China, Singapore, South Korea and Taiwan. The report has concluded that with the statistic of 65 % of the mobile user sending text messages everyday, SMS will continue playing an important role as the most popular mobile data application [2].

In April 2003, hongkong.com has successfully acquired Newpalm (China) Information technology Co., Ltd, a leading short message service (SMS) mobile software platform developer and application service provider in China, to provide additional direct connectivity for four provinces which are Hebei, Yunnan, Gansu and Xinjiang. Obviously, the SMS application will continue providing its influence to the penetration of market rate of mobile services in the next few years [3].

Although mobile messaging is having great influence in daily life, unfortunately, most of the communication is unsafe. The message sent from the mobile device will store at the message centre of associate network provider. The message will travel across different base station in unprotected manner. This means there is an opportunity to allow the middle man attack on those confidential messages. Moreover, the mobile phone can be accessed by other user in the case of phone sharing or lost. Thus, it leads to the introduction of symmetric encryption on SMS, where both sender and recipient hold the same secret key for encoding and decoding the message.

Previously, symmetric encryption uses same key for both side communication. There is high possibility the key will be known to the public. Even it is simple and fast, but it has problem on key distribution and thus decreases the reliability on service. As a result, it is not suitable be applied for the critical application like SMS.

Whitfield Diffie and Martin Hellman (1976) proposed the notion of public-key cryptography [4]. There are two mathematically related keys, which known as public key and private key, used in the message encryption. The key pairs are generated by using the asymmetric cryptography algorithm and kept secretly. These early cryptography does not request the authentication from the sender. As a result, it leave to middle man attack even it is sufficient for preventing the eavesdropping activity. The following is the protocol for generating encryption key using public-key cryptography [5].

1. The sender, Sam and recipient, Ryan will agree on a prime number p and base g.

2. Sam then picks an integer a and sends the $g^{a} \bmod p$ to Ryan.

3. Ryan also picks an integer b and sends the $g^{b} \bmod p$ to Sam.

4. Both of them then start the computation as below:

   Sam: $(g^{b} \bmod p)^{a} \bmod p$ (1)

   Ryan: $(g^{a} \bmod p)^{b} \bmod p$ (2)

5. The result of computation will give the same value for Sam and Ryan.

* *The value of a, b, and* $g^{ab}=g^{ba}$ *are kept in secret.*

In other to distribute the symmetric key, the public key cryptosystem is used. The most popular mathematic algorithm used is RSA. The algorithm will generate two keys, which is public key and private key, by manipulating two prime numbers with a series of computations. The public key will distribute publicly and the private key will keep secretly by the user. This is to ensure that the secure message, which encrypted using recipient's public key, will be read by the targeted person, with the private key to decrypt the encryption. Furthermore, the public key can be used to verify the digital signature which is signed with the sender's private key.

2 m-PKI

Currently, most of the mobile phone do not offer any specific security features on SMS/MMS. By implementing PKI in SMS/MMS architecture, the problem such as eavesdropping, tampering, and impersonation [6] can be overwhelmed. The secret end-to-end encryption will ensure the message to be read by the right person only. Personal or corporate private and confidential message can be retained.

Furthermore, concept of using public key and private key for message encryption and decryption is easy for public to understand, accept and use. The implementation cost of *M*-PKI is cheap and will not cause any major issues on violating intellectual property right. For addition, this solution does not involve any hardware installation or additional device.

Since Public Key Infrastructure (PKI) is a proven solution for normal secure Internet communication encryption, it should be implement on mobile SMS/MMS. Besides that, *M*-PKI provides classification on SMS/MMS which sender can choose to send normal SMS/MMS, SMS/MMS with password protection, and PKI SMS/MMS.

On the other hand, most of the mobile PKI solution has problem on managing the key distribution. Some proposal suggested smart cards [7], software tokens [8] or long password [9] but there is possibility of losing the private key to the public when phone is lost. Additional verification process is applied for retrieving PKI certificate has been introduced to overcome these issues.

2.1 PKI on Java

The idea of using mobile PKI was raised by Tadashi Kaji (2004) when mobile communication becomes so important ever than before [10]. The concept of applying PKI encryption to mobile SMS/MMS has introduced an alternative way to communicate in a private and secure manner.

Limor Elbaz (2002) has mentioned the idea of using public key cryptography in mobile phones [6]. The design is named as CryptoCell^{TM} . Its architecture consists of five layers, which are hardware layer, firmware layer, API layer, protocol layer and application layer. User will be provided a pair of key (public key and private key) for information encryption. These solution arise the issues such as theft and phone lost which will cause the disclosure of private key and confidential information.

Java based PKI on mobile SMS has introduced by Marko Hassinen (2006) [11]. Symbian and J2ME are used as the development platform. Unlike the smart card solution, this system, build on WMA and MIDP 2.0 (Mobile Information Device Profile), can run on all java enabled mobile devices. Unfortunately, no classification on mobile messaging is provided in this solution. The issue in this purposed system is how to safely store the private key in the mobile phone.

IPCryptSim (2006) [12] starts the smart card solution for mobile PKI messaging. The user private key, authentication password and IPCryptSim application are stored in the SIM card. This solution has involved the cooperation and service agreement with the network provider. The advantage of IPCryptSim is it can be implement on all types of mobile phone if or without the Symbian platform or MIDP 2.0.

3 m-PKI Solution

3.1 *M* –PKI Architecture

M–PKI architecture consists of *M*–Certificate Authority (*M*CA), *M*–Certificate Management System, and *M* –certificate database. Please refer to Fig.1. The applicant first must apply a digital certificate with the certificate authority before start using the *M* –PKI application. After all the verification processes are done, the certificate authority will issue the certificate to that particular applicant. The certificate then be stored at the server database and managed by certificate management system.

The *M* –PKI's user can check the status for his/her and recipient's certificate from time to time. *M* –PKI messaging will require the sender to attach the recipient's public key for encryption purpose. For first time communication, sender can download the public key from the *M* –PKI directory at server. The certificate management system will retrieve the correspondence certificate from database once receive the request from *M* –PKI directory. If the certificate has been revoked, the messaging communication will not be established.

3.1.1 *M* –PKI user

All *M*–PKI users have to possess a Java-enabled phone, which allies to Open Mobile Alliance (OMA) standard, to install *M* –PKI application. OMA support Java interface such as Mobile Information Device Profile (MIDP) 2.0. It is as part of J2ME and used by mobile device to run Java applications. Nokia Presence Server 1.0 is based on the OMA Instant Messaging [13] and Sony Ericsson mobile messaging also supports this standard [14]. The PKI algorithm will be built in MIDlet using the Lightweight API from the Legion of Bouncy Castle, which provides

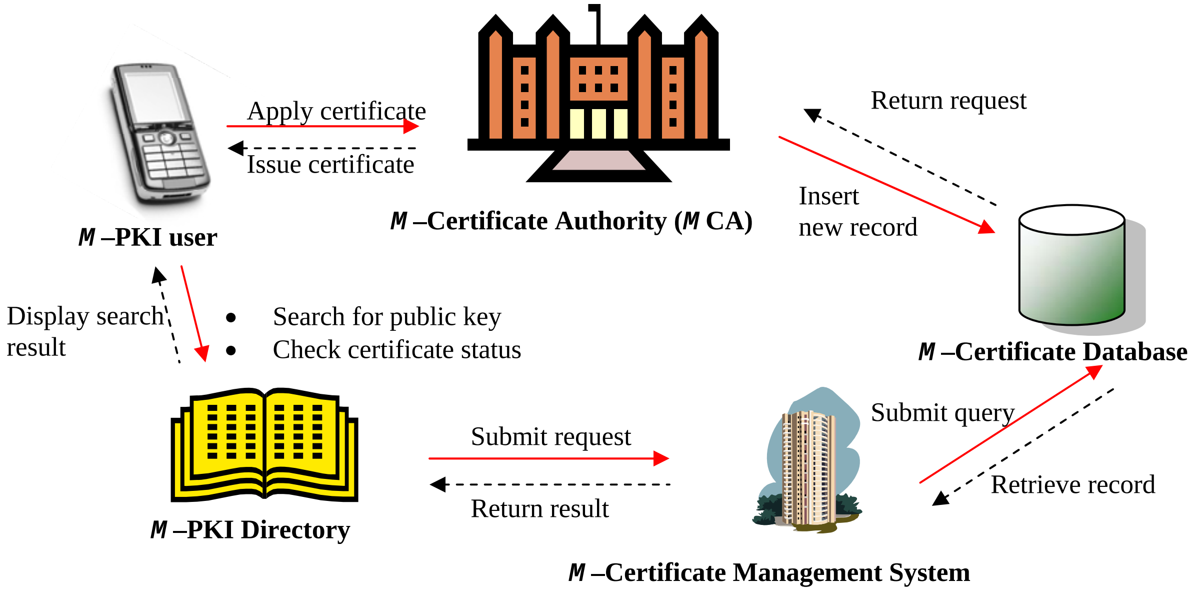

Fig.1 : *M* –PKI Architecture

cryptographic algorithms to run in J2ME environment [15].

Secondly, *M*–PKI users have to register with the *M*–Certificate Authority (*M*CA) in order to apply the mobile digital certificate. Once the certificate has been issued, *M*–PKI users can install it into the phone. To establish confidential SMS communication, M–PKI users have to visit the *M* –PKI directory. This directory will provide the information for all *M* –PKI users' certificate and its status. It is the responsibility of the *M*–PKI user to check the validity of the recipient's certificate.

3.1.2 *M* –Certificate Authority (*M*CA)

M–Certificate Authority (*M*CA) will issue a digital certificate for each user after completing all verification processes. The user personal particular such as name, identity number (IC), contact number, email, and address will be stored together with the certificate at the server database (*M*–Certificate Database). The *M*–PKI user can install the certificate when it has been successfully generated by the *M*CA.

3.1.3 *M* –Certificate Database

All the contact information and mobile digital certificate are stored here. The certificate contains the information about the *M*–PKI user's public key, algorithms used, date of validity, issuer's name, date of creation, continuous number, signature of *M*CA [16], and etc.

3.1.4 *M* –Certificate Management System

This system is used to manage all issued digital certificated. It processes the request receive from *M*–PKI directory and retrieve the associate record from the *M*–Certificate database. Besides, it also handles those expired certificate and lost certificate report in order to renew the correspondence certificate.

3.1.5 *M* –PKI Directory

This is a directory used to store PKI critical component such as certificate, all *M*–PKI users contact information and other PKI information and policies. All users' public key and the validity period of the certificate are published here. The search key is using the correlated phone number.

3.2 *M* –PKI Application

In cryptography, a public key infrastructure (PKI) is an arrangement of a pair of keys which is public key and private key. Public key will represent the identity of that user. To establish secure communication, the sender is required to sign the message with own private key. This encrypted message will then encrypt with recipient public key, which is available at repository. Recipient has to decrypt the message using own private key. In other words, only the right person with the correct key can read the message content and even the sender also not able to reach this message. Please refer to Fig. 7 in next section (M–PKI scenario) for the detail of message exchange.

To increase the security of mobile SMS/MMS, information will be classified into three categories which are public, internal and confidential. Ordinary SMS/MMS which allow for public access will be classified as normal. No authentication is required for this public message and it can be accessed by anybody. This is to ensure the performance on sending non-classified information.

For company internal communication, symmetric encryption will be applied to the message. PKI encryption only applies for confidential use. Confidential is refers to the type of message that contain highly sensitive information such as political or legal issues, marketing information, and company access code. This message will be encrypted by PKI algorithm and additional verification procedure. Please refer to Fig.2 for the details of information classification. The total message size in GSM (Global System for Mobile Communications) network is limited to 160 characters [17]. Therefore, confidential SMS will split into two messages and reassemble when reached at the recipient phone.

The major different between confidential message and internal message is the algorithm used for encryption. The internal SMS uses a symmetric key that previously agreed by both sender and recipient. However, two different key, which are public key and private key, are used for the confidential (PKI) SMS. Additional authentication process will be required for confidential message compare with internal SMS. This will decrease the performance on sending and retrieving message but it increases the reliability and security of message delivering to targeted person. M–PKI user should not forward the content of message, which labeled as confidential, to third party or expose the message to the public.

3.2.1 M–PKI Scenario

M–PKI is an application for secure mobile communication using SMS/MMS. M–PKI messaging flow is shown in Fig.3. In normal mode, M–PKI user can send SMS for daily communication which is straightforward. No protection is provided for this category. Please refer to Fig.4.

When a sender wished to communicate in a private manner, he/she should start the M–PKI application. First, the sender needs to select the internal SMS. As sending normal SMS, sender has to attach the recipient’s contact number and compose the message. After that, sender needs to provide a password which is agreed by the recipient. Then the process is completed when the send button is pressed. Please refer to Fig.5.

The encryption algorithm used is Advanced Encryption Standard (AES). AES was announced by National Institute of Standard and Technology (NIST). The 128 bit encryption length is more than enough to protect the information up to the secret level [18].

When the sender chooses to enter the confidential mode, he/she needs to fill in the phone number and associate public key for the recipient. The sender can access to the server for first time communication. The server also has the directory to show the status of digital certificate for all public key holders. Please refer to Fig.6 for illustration. It is important to remind that the sender has the responsibility on determine the validity of the recipient’s public key for legitimate purpose. In mobile device, client’s private key is securely stored in the mobile device.

M –PKI uses the library downloaded from Bouncy Castle to generate key pairs. Both public key and private are generated by the RSAKeyPairGenerator class. The following is the coding for key generation.

```
BigInteger pubExp
= new BigInteger("1001", 16);
SecureRandom sr = new SecureRandom();    (3)
RSAKeyGenerationParameters
        RSAKeyGenPara =
 new RSAKeyGenerationParameters
        (pubExp, sr, 512, 80);           (4)
RSAKeyPairGenerator RSAKeyPairGen
= new RSAKeyPairGenerator();             (5)
RSAKeyPairGen.init(RSAKeyGenPara);       (6)
AsymmetricCipherKeyPair keyPair =
        RSAKeyPairGen.generateKeyPair(); (7)
```

By calling generateRSAKeyPair(), the class will automatic generate the public key and private key. Then, the getPublic() is to extract the generated public key and getPrivate() for private key. These two methods are from generateRSAKeyPair() class.

The **public key** consists of the modulus ***n*** and the public (or encryption) exponent ***e***. The **private key** consists of the modulus ***n*** and the private (or decryption) exponent ***d*** which must be kept secret [19]. The following mathematic equation shows how the RSA algorithm encrypts and decrypts the message. The message will encrypt by the public key and successfully decrypt if private key is provided.

For encryption,

$$c=m^e \bmod n \tag{8}$$

For decryption,

$$m=c^d \bmod n \tag{9}$$

where m = message, c = message with encryption

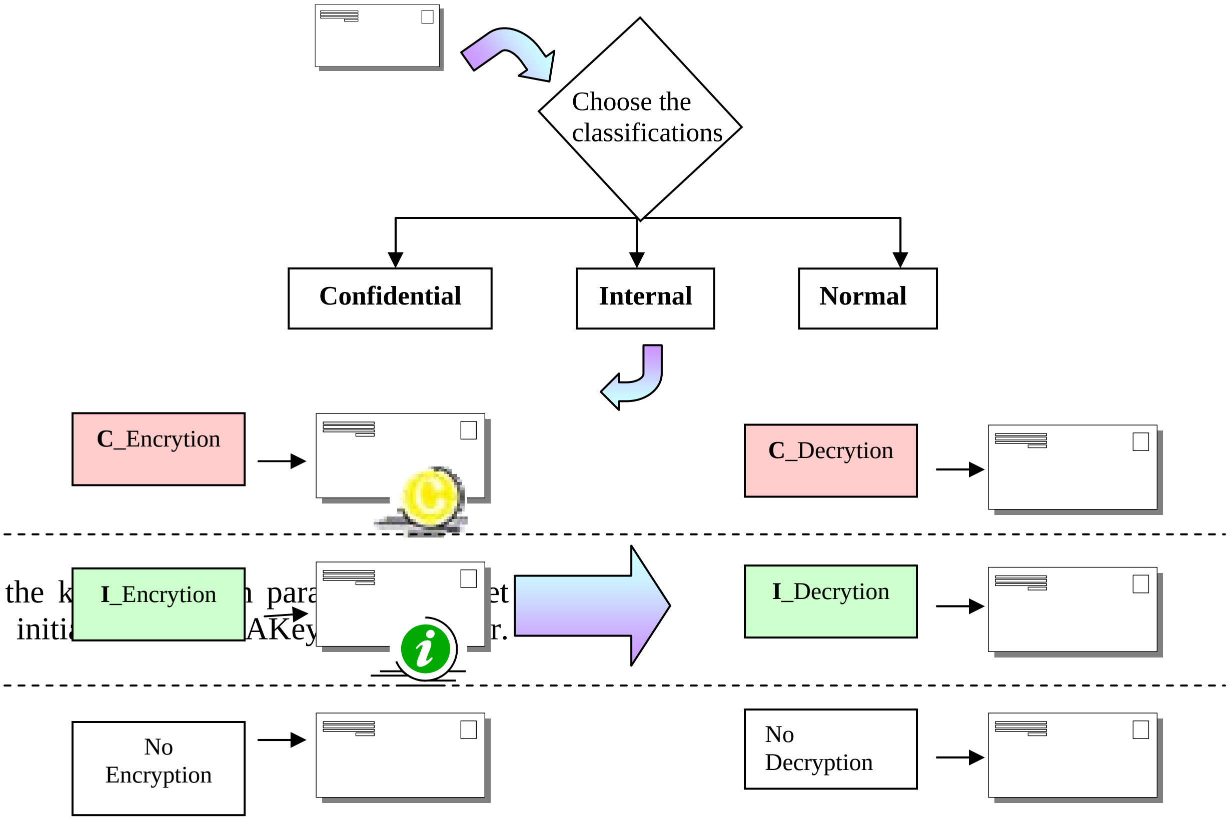

Fig. 2: Message Classification

First, the k para et and then initi AKey r.

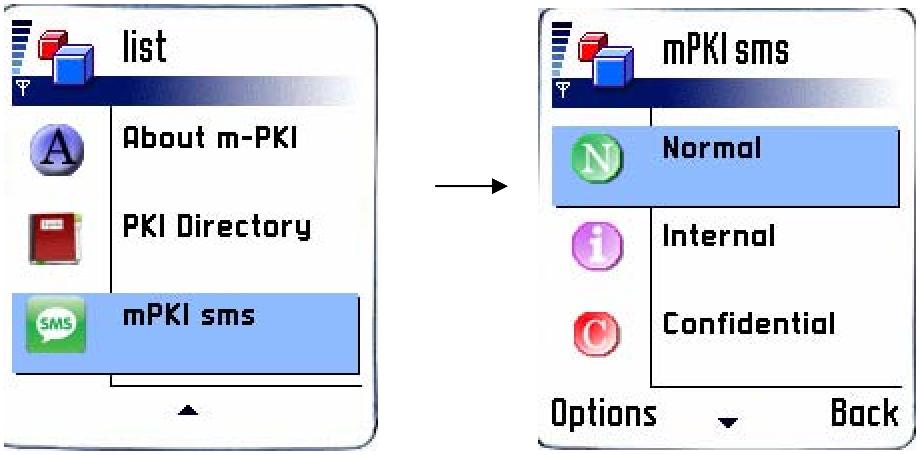

Fig.3 : M –PKI messaging flow

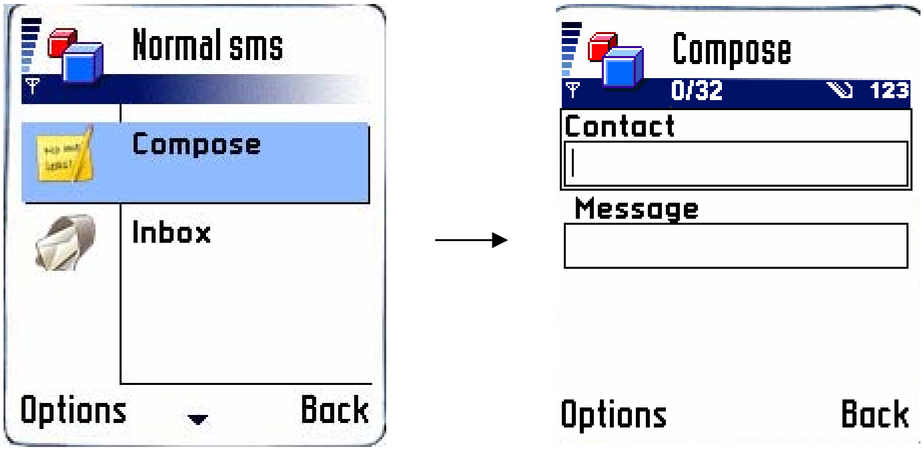

Fig.4: Normal SMS flow

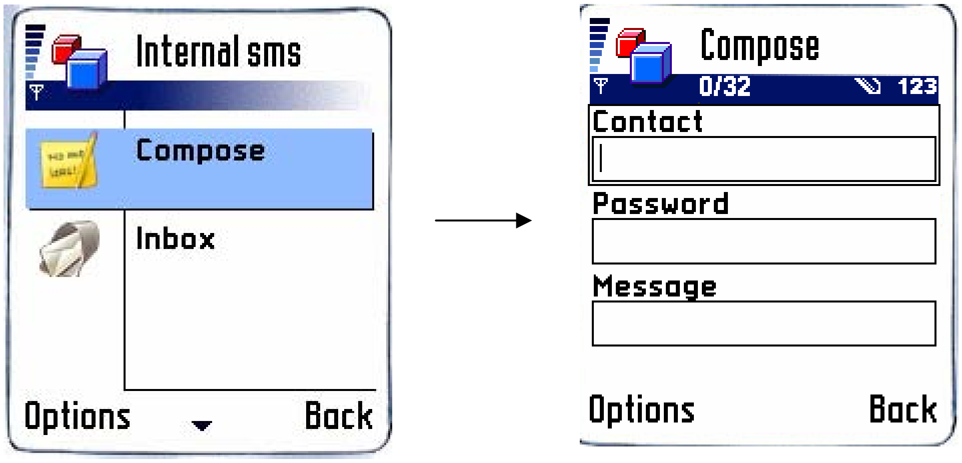

Fig.5: Internal SMS flow

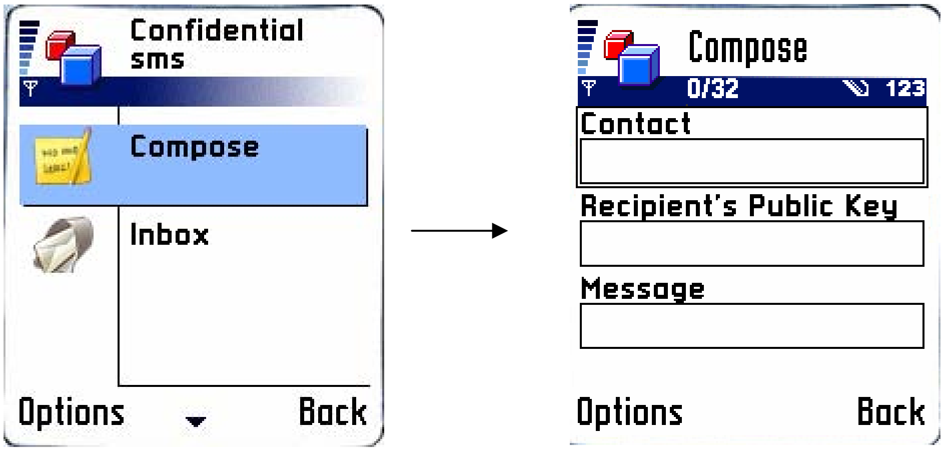

Fig.6: Confidential SMS flow

The following diagrams will illustrate the scenario on sending and replying PKI SMS. Sam wants to send SMS to Ryan in a confidential manner, so he choose confidential mode. For first time communication, Sam need to visit *M* –PKI directory to search for Ryan's public key and verify the validity period of Ryan's digital certificate. After that, Sam has to attach his private key to the message. Then, Ryan will decrypt the message using his own private key to reach the message. Please refer to Fig.7. The reply SMS scenario is same with the send SMS scenario. If Ryan has Sam's public key previously stored in the phone, then he does not need to visit the *M* –PKI directory.

3.3*M* –PKI Strength

Currently, most of the mobile PKI solution does not offer the classification on messaging. The SMS/MMS will be categorized into three categories which are normal SMS (no encryption), internal SMS (symmetric encryption), and confidential SMS (PKI encryption). *M*–PKI users are free to choose which classes of encryption wish to apply and even no protection for the SMS.

Besides, the contact list in the *M*–PKI application will offer the convenient on searching and storing other *M*–PKI users' contact information. For example, Sam and Ryan have to agree on the shared password for this symmetric encryption in first time communication and store it in the correspondence contact list. Then, Sam can send the internal SMS by selecting the name of Ryan in the contact list. The phone number and shared password will display automatically. This is to prevent both of them forgot the password. The confidential SMS which uses private key and public key will apply the same protocol as internal SMS

The inbox of *M*–PKI can used to store encrypted message. The password will be requested for internal SMS and private key for confidential SMS when retrieving the SMS. This is to prevent unauthorized person attempt to access the private SMS, as described by the mentioned cases such as phone sharing or phone lost.

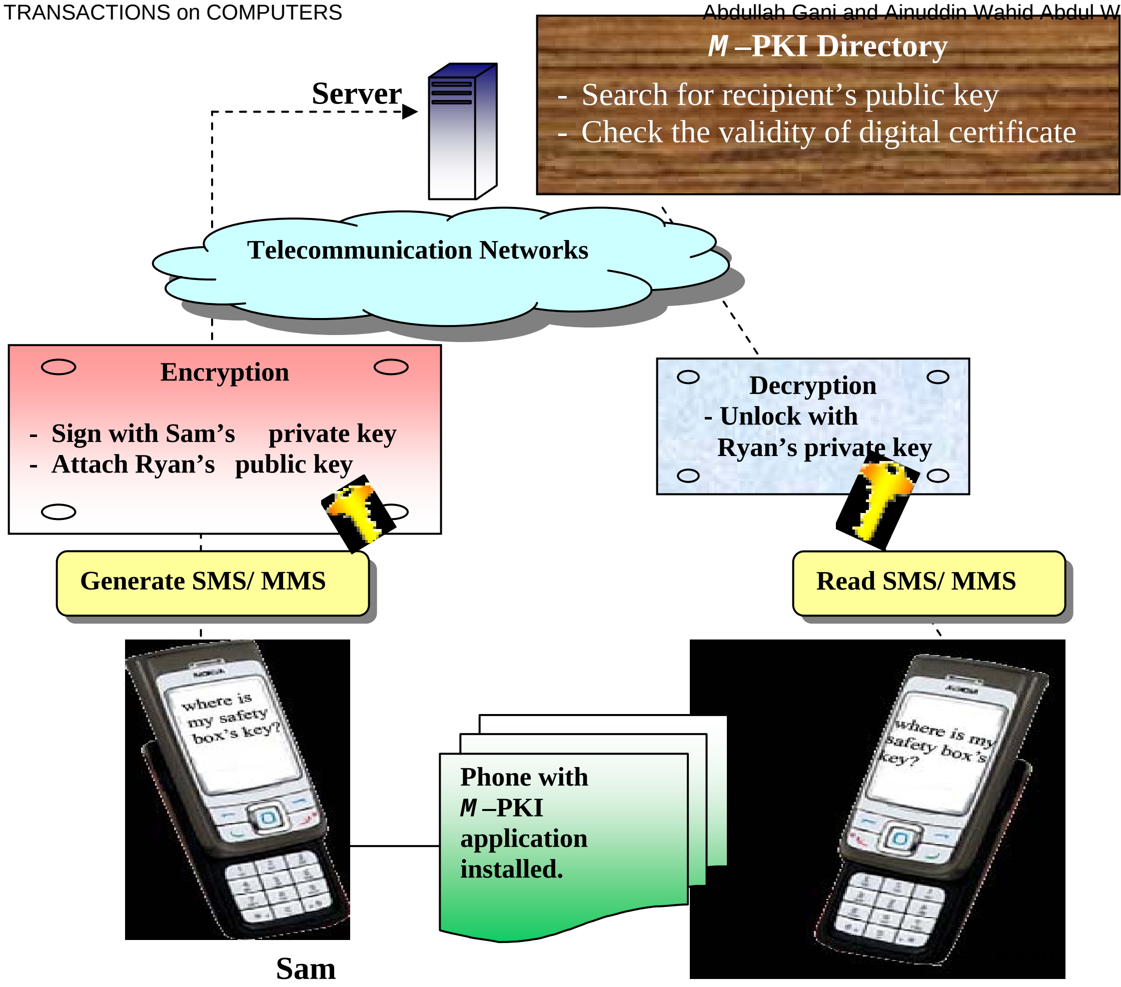
M –PKI Directory
- Search for recipient’s public key
- Check the validity of digital certificate
Server
Telecommunication Networks
Encryption
- Sign with Sam’s private key
- Attach Ryan’s public key
Decryption
- Unlock with Ryan’s private key
Generate SMS/ MMS
Read SMS/ MMS
where is my safety box’s key?
where is my safety box’s key?
Phone with M –PKI application installed.
Sam

Fig.7: Send Message Scenario

4 conclusion

The solution for secure wireless communication in the future will be mobile PKI. The demand for secure mobile encryption will become increasingly important because too many applications have been built for mobile phone. Besides that, the PKI technology is easy to understand and accept by public. For addition, the implementation cost is economic and it is easy to install. However, the solution still can be improved by introducing biometrics feature for user authentication. This technology is expensive and causes issue on privacy. This could be solved by recommending new policy control but requiring extra effort on standardizing the policy used by Telecommunication Companies and trusted third party such as certificate authority. *M*-PKI can be improved from time to time and it will accomplish all the goals for why it was built for sure.

5 Future work

The significant use of mobile communication has raised the need to communicate privately. The proposed solution can be used for further research in terms of quality improvement and performance enhancement.

Public Key Infrastructure (PKI) is a proven solution for secure communication encryption. This concept is applied in this paper to offer security control on wireless communication. Further effort on transforming the *M*-PKI from mobile SMS/MMS into various wireless applications such as remote sensing and control on home appliances or hardware peripheral [20] via handheld devices is encouraged. Besides that, intellectual property right can be protected by authenticating the web user for information download especially for entertainment and business products. For addition, medical services such as billing system, appointment booking and patient's record access [21] can be implemented via m-PKI.

Introducing biometrics feature such as voice and keystroke in encryption and decryption process will be the further study for this area. This feature will ensure the future electronic government on implementing mobile PKI as an alternative solution for various alliances. For example, renew road tax and insurance, mobile payment and even for collecting votes during public election.

Research on applying PKI in voice communication will be interesting and meaningful. The voice communication is the main attraction in mobile and internet applications. The repudiation in PKI will help in verifying the identity of target party. The recorded conversation can be used as legal evidence because all parties involved could not deny the content and their participation on that conversion.

In future, perhaps new features or applications will be carried out for education purpose. The verification for student identity during examination, academic assessment and personal information update could be done using mobile PKI.

Besides that, there is a demand on standardize the policy on key management. Building trust and maintaining trust relationship among different parties is difficult. The effort on applying PKI in various field depend on government policy control.

References:

[1]. Mobile Data Association (Press Release), "The Q1 2008 UK Mobile Trends Report," February 4, 2008. [Online]. Available: http://www.themda.org/documents/PressReleases/Switch/MDA_Q1_2008_UK_mobile_report.pdf. [Accessed March 13, 2008].

[2]. Telecom Asia, "SMS is top service for Asian mobile phone users," March 3, 2006. [Online]. Available: http://www.feedsfarm.com/article/447aea1518911c20d63c0c08dfe0ce00e6ad59ae.html. [Accessed April 18, 2008].

[3]. C. Jane, "Mobile SMS Unit Increases Direct Connectivity With Local Mobile Network Operators in China," October 14, 2003. [Online]. Available: http://www.inc.china.com/admin/upload/newsroom/press/ep031014.pdf. [Accessed April 18, 2008].

[4]. W. Diffie and M. Hellman, "Multiuser cryptographic techniques," in *AFIPS Conference*, 1976, Volume 45, pages 109-112.

[5]. RSA Laboratories, "Chapter 3 Technique in Cryptography: What is Diffie-Hellman?," May 11, 2008. [Online]. Available: http://www.rsa.com/rsalabs/node.asp?id=2248. [Accessed May 11, 2008].

[6]. L. Elboz, "Using Public Key Cryptography in Mobile Phones," Discretix Technologies Ltd, October 2002. [Online]. Available: http://www.discretix.com/PDF/Using%20Public%20Key%20Cryptography%20in%20Mobile%20Phones.pdf. [Accessed April 12, 2007].

[7]. T. Chanson and C. Tin-Wo, "Design and Implementation of a PKI-Based End to End Secure Infrastructure for Mobile e-Commerce", *World Wide Web*, vol. 4, no.4, pp 235-253, December 2001.

[8]. T. Kwon, "Virtual Software Tokens – A Practical Way to Secure PKI Roaming," in *Lecture Notes in Computer Science*, Vol. 2437, pp 288-302, 2002.

[9]. R. Sandhu, M. Bellare and R. Ganesan, "Password-Enabled PKI: Virtual Smartcards versus Virtual Soft Tokens," in *1st Annual PKI Research Workshop*, pp 89-96, 2002.

[10]. Tadashi Kaji, "Mobile PKI Framework (1): HITACHI-SDL," March 2008. [Online]. Available: http://www.sdl.hitachi.co.jp/english/people/pki/index01.html. [Accessed March 22, 2008].

[11]. M. Hassinen, “Java based Public Key Infrastructure for SMS Messaging,” in *2nd Information and Communication Technologies Conference*, 2006, pp 88- 93.

[12]. IPCS Group, “IPCryptSim SMS Encryption,” March 22, 2008. [Online]. Available: http://www.ipcslive.com/pdf/IPCSmbank.pdf. [Accessed 22 March 2008].

[13]. “Forum Nokia Style Guide Version 3.0,” March 2003. [Online]. Available: http://www.differnet.com/crose/Samples/CRose-NokiaStyle.pdf. [Accessed February 22, 2008].

[14]. Sony Ericsson, “MMS Developers’ Guidelines Feature Phones,” May 22, 2008. [Online]. Available: http://developer.sonyericsson.com/site/global/docstools/messaging/p_messaging.jsp. [Accessed May 22, 2008].

[15]. “The Legion of Bouncy Castle,” Feb.8, 2008. [Online]. Available: http://www.bouncycastle.org. [Accessed February 8, 2008].

[16]. M. Petraschek, “Public Key Infrastructure for Mobile Devices,” Apr, 2007. [Online]. Available: http://www.ftw.at/ftw/events/telekommunikationsforum/SS2004/SS04docs/040422.ppt. [Accessed April 12, 2007].

[17]. C.M. Sarraf, et al., “Measuring QoS for GPRS Mobile Networks,” in *4th WSEAS International Conference on Telecommunications and Informatics, March 13-15, 2005, Prague, Czech Republic*, pp 493-257.

[18]. CNSS, “National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information,” *CNSS Policy No. 15*, Fact Sheet No. 1, June 2003. [Online]. http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf.

[19]. J. Alfred, C. Paul and A. Scott, *Handbook of Applied Cryptography*, CRC Press, 1996, pp 283-319.

[20]. R. Pandhi, et al., “A Novel Approach to Remote Sensing and Control,” in *6th WSEAS International Conference on Artificial Intelligence, Knowledge Engineering and Databases, February 16-19, 2007 , Corfu, Greece, 2007*, pp 540-280.

[21]. C. Toma, et al., “Secure Mobile Electronic Card used in Medical Services,” in *Applied Computing Conference, May 27-29, 2008, Istanbul, Turkey*. WSEAS Press.