Usability and Performance of Secure Mobile Messaging: 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: Human life style change substantially when the cellular technology goes commercial. Short Messaging Service (SMS) and Multimedia Message Service (MMS) play important roles in our daily life. The recent report carried out by Mobile Data Association (MDA) [1] shows that the yearly growth of SMS and MMS achieves 30 percent from year 2007 to 2008. Conventional SMS/MMS does not provide any protection on the text message sent. It causes the security threats such as privacy and message integrity. Mobile users seek for the solution to allow them to exchange confidential information in a safe environment. This leads to the implementation of M-PKI, which is an application that secures the mobile messaging service by using public key infrastructure (PKI). This new approach allows the end-user to send private and classified message via SMS. Besides, M-PKI offers message classification. This feature is specially designed to meet various user requirements on the level of security and performance. The usage and performance of M-PKI messaging in performing encryption and decryption process are tested on selected java-enabled phone.

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

1 Introduction

People nowadays used to bring the cell phone wherever and whenever they are. There are 224 million units mobile phones sold worldwide in the first quarter of 2006 [2]. A survey has been carried out by the iGR (September, 2006) and found that the most commonly used mobile device among mobile worker is cell phone [2]. This figure points out a truth which is the human communication has evolved from the wired telephony to the wireless telecommunication. In other words, the handheld device has successfully replaced traditional telephone to become the most popular wireless communication tools.

Recently, mobile users depend greatly on SMS or MMS to communicate with the people around. SMS and MMS fulfil almost the entire user requirements on daily communication. For example, information exchange via text, picture, voice and video. All this services are now available in mobile messaging system. It is simple, easy, and convenience to use. Most of the mobile users are satisfied on the usability and performance of the mobile messaging system. According to the report [1], the text messages being sent per week in United Kingdom (UK) exceeded 1.4 billion in year 2008. Apparently, society has reached to a state that without SMS or MMS would be a major disruption.

Unfortunately, most of the mobile messaging communication is unsafe. The enterprise Information Technology (IT) managers in United State (US) concern the most are the user authentication and the encryption of data, which achieve the top and second ranking in the survey [2]. The wireless security especially in mobile telecommunication is hard to assure the mobile user on preventing the issues such as eavesdropping, tampering, and impersonating. The message sent travels across the network is in an unprotected manner. It provides an opportunity for the third party such as the administrator of message centre or the adversary to reach to the message. Moreover, the sensitive data can be accessed by unauthorized user when the phone is lost or shared. Therefore, the need of message encryption is emerging.

M–PKI classifies the mobile text message into three categories which is normal, internal, and confidential. Ordinary SMS is classified as normal because it allows the public to access. It does not require authentication because we have to ensure the performance in sending non-classified information. For private communication such as company internal announcement, discussion, and meeting notice, symmetric encryption is applied. Asymmetric encryption (also know as PKI encryption) only applies for confidential use. Confidential SMS is specially design for those messages that contain highly sensitive information such as political or legal issues, marketing information, or company access code. Besides, it also helps the mobile users to verify the content of SMS sent by the telecommunication company for the purpose of promotion and competition. The concept of public key and private key is used. *M*–PKI user is not able to store the message or forward the confidential SMS to the third party because the message is destroyed after being read. This security feature is to preserve the confidentiality of the message and the privacy of sender and recipient.

2 Cryptography

Knudsen (1998) [3], the writer of Java Cryptography, has described that cryptography is the art of secret writing. Generally, cryptography is one of the branches of mathematic. It uses algorithm to encrypt the information and transforms it to unreadable format. The reverse process is decryption. It always used for authentication, integrity and confidential purpose. Normally, cryptography is applied in the network security and data protection such as secure transaction, email, and important file. Symmetric and asymmetric algorithms are two famous algorithms in cryptography.

The safest way to ensure all confidential data, file and message are unreachable by adversary or unauthorized person is encryption. Encryption is the conversion of plain text into unreadable cipher text. This conversion is done after undergo a series of complex mathematical transformational steps. Therefore, it can prevent eavesdrop activity. The security of encryption depends on the decided key length and algorithm used. According to National Security Agency (NSA), the key length falls between 192 to 256 bits is considered as TOP SECRET level [4]. If the encryption algorithm is more complex, the produced cipher text may be harder to be broken. However, the implementation cost will be more expensive and decrease the speed of the performance.

The procedure that needs to transform the cipher text to the original message is called decryption. The actual message can only be read when the correct key is given. Same key is used for symmetric encryption and decryption. Furthermore, same algorithm that applies for encryption must be used for decryption. Asymmetric encryption/decryption also execute in the same manner.

2.1. Advanced Encryption Standard (AES)

Vincent and Daemen (1998) have published the new symmetric algorithm which is Advanced Encryption Standard (AES). It is highly recommended by National Institute of Standards and Technology (NIST) as more effective algorithm than DES and Triple DES. AES, or also known as Rijndael, is finalized in November 2001 as Federal Information Processing Standards (FIPS) 197 [5].

AES supports a fixed block size of 128 bits and the available key size are 128, 192, 256 bits. Until year 2006, an attack named as *side channel attacks* has made successful attempt to break the implementation of AES. This attack is against the systems with AES implementations that accidentally leak data. Since it does not try to break the fundamental cipher, the security strength of AES is retained. Based on the testing [6], time needed to crack the AES key is 149 trillion years, which is considered as lifetime. The time used for performing encryption/decryption for AES is also shorter compared with Triple DES.

2.2. RSA

Asymmetric encryption is based on public key and private key. These two keys are generated together in pair. The private key cannot be regenerated from the public key. This characteristic allows the public key to be distributed openly to anyone. Moreover, it can convince the user that the recipient is the target person. This is because the encrypted message can only be decrypted by the private key, key that formed in pair with the correspondence public key. In addition, digital signature provides authentication and protects the integrity of message against tampering. The most widely used public-key cryptography algorithm is RSA cryptosystem which security is based on the intractability of the integer factorization [7] (Alfred, Paul & Scott, 1996:285). In *M*–PKI, it has been used to provide both secrecy and digital signatures on mobile messaging.

RSA cryptosystem is selected as the public key encryption algorithm for *M*–PKI confidential SMS due to its proven security strength, performance and simplicity. The disadvantage of ElGamal encryption is that the produced cipher text is twice as long as the corresponding plaintext (message expansion by a factor of 2) [7]. Besides, it needs a generator as the component of public key. The computed generator is weak and reduces the security strength of the key pair.

To generate the RSA key pair, the following computation is taken [7]:

1. Elect two large random (and distinct) primes p and q.
2. Compute $n = pq$ and $\varphi = (p - 1)(q - 1)$.
3. Select a random integer e, $1 < e < \varphi$, such that $\gcd(e, \varphi) = 1$.
4. Use the extended Euclidean algorithm to compute the unique integer d, $1 < d < \varphi$, such that $ed \equiv 1 \pmod{\varphi}$.
5. The generated public key is (n, e), where n is modulus and e is encryption exponent.
6. The private key is d where d is also the decryption exponent.

Example: Entity D chooses the primes p = 2357, q = 2551.
Computes n =pq = 6012707 and
$\varphi = (p-1)(q-1) = 6007800$
D chooses e = 3674911 and, using the extended Euclidean algorithm, finds d = 422191 such that $ed \equiv 1 \pmod{\varphi}$.
D's public key is the pair (n = 6012707, e = 3674911), while D's private key is d = 422191.

Let say entity C wishes to send message m to entity D secretly. The message will undergo several computations to produce the cipher text [7].

1. Obtain D's authentic public key (n, e).
2. Compute cipher text $c = m^e \bmod n$, where m fulfil the condition $0 \le m \le n\text{-}1$.

Example: Let message **m = 5234673**, C computes
$c = m^e \bmod n = 5234673^{3674911} \bmod 6012707 = 3650502$ and sends this to A.

In order for D to transform the cipher text to plain text (message), following procedure is needed.

1. D uses the private key d to recover message $m = c^d \bmod n$.

$$\begin{aligned} \mathbf{m} &= c^d \bmod n \\ &= 3650502^{422191} \bmod 6012707 \\ &= \mathbf{5234673} \end{aligned}$$

If D wants to send a signed message to C, the RSA digital signature schemes is as below (Alfred, Paul & Scott, 1996:434):

1. Compute □ = R(m), where *m* fulfil the condition $0 \leq m \leq n$-1.
2. Compute s = □ ^{d} mod n.
3. A's signature for message *m* is *s*.

Example: Let message □ = **3650502**, C computes s = □ ^{d} **mod n**

= 3650502^{422191} mod 6012707

= 5234673 and sends this to C.

Then, C can verify D's signature and recover the message *m* by following the computation below (Alfred, Paul & Scott, 1996:434):

1. Get A's public key (*n*, *e*).
2. Compute □ = s^{e} mod *n*.
3. Verify that □ ∈ M$_{R}$; if not, reject the signature.
4. Recover $m = R^{-1}$(□).

Example: To verify, C computes

□ **= s^{e} mod *n***

= 5234673^{3674911} mod 6012707

= 3650502

3 System design and performance testing

M–PKI has two major modules, which are MCA and M–PKI's user. The main responsibility of MCA is the key management. The role of MCA is clearly illustrated in Fig. 1(a) while the actual interface is shown in Fig. 1(b). MCA will generate the key pair when new user has subscribed for the M–PKI application. The used *include* relationship in the diagram refers to the automatic process in saving the key pair to the database after the key pair generation process. The function is set for key management and system back up if the user's phone is lost. Later, the key pair is sent to the user via M–PKI messaging service and stored in the user phone.

The application user can accountable on the *M*CA in the key distribution. In cryptography, public key can be distributed freely. The *M*-PKI's application is designed in such a way that *M*CA and the users are allowed to send the corresponding public key to those who request for it. On the other hand, only the *M*CA is allowed to send the private key to authorized user for successful registration or in a special situation such as switching to a new phone or key corruption. Both keys are sent via *M*-PKI's messaging service.

M-PKI's user focuses on the *M*-PKI's messaging services such as the function of sending and reading text message. The strength of *M*-PKI is the message classification which allows user to send classified message. The user requirements for system functionality have been captured by the use case diagram in Fig. 2. The *generalization* relationship shows three specific messages, which are normal SMS, internal SMS and confidential SMS, that supported by the *M*-PKI's messaging service. Users are free to choose the messaging services as planned according to their need.

User has to compose the message first before trying to send that particular message. The encryption process is applicable for internal SMS and confidential SMS. However the signing process is only available for confidential SMS. Internal SMS is specifically for private message such as meeting schedule and venue, identity number (IC No.), and booking number for movie ticket. This type of SMS provides password protection (symmetric encryption) to the message. Both the sender and recipient have to agree on the secret key used for message encryption and decryption. The encrypted message travels in the GSM network in an unreadable format. The recipient needs to provide the correct password in order to read the content of message. The privacy of the user is protected.

Unfortunately, the symmetric encryption has a problem on key distribution and it is not difficult to break the encryption when large computation power is available today. Therefore, PKI takes place in improving the current encryption and decryption process. The confidential SMS applies the concept of PKI on mobile messaging service. Every user has a pair of key, which are public key and private key. The public key can be distributed publicly to every M-PKI's user but the private key has to be kept secretly on the mobile phone.

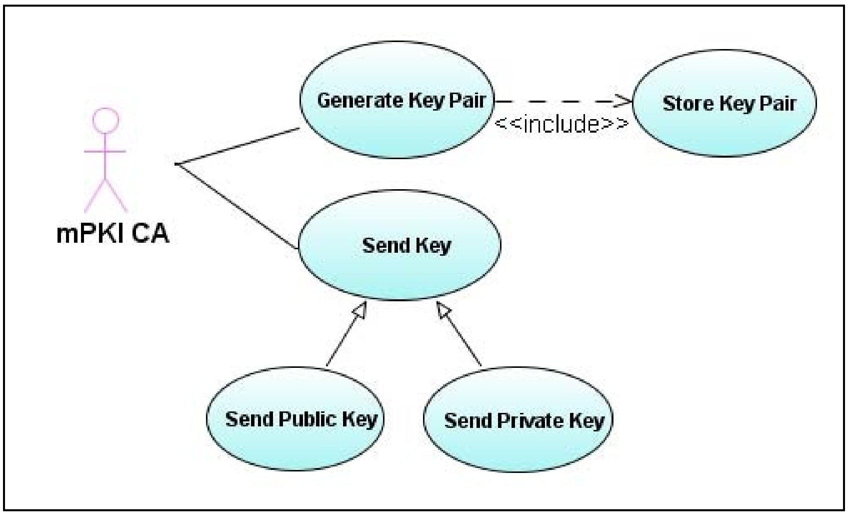


Fig. 1(a): MCA Use Case Diagram

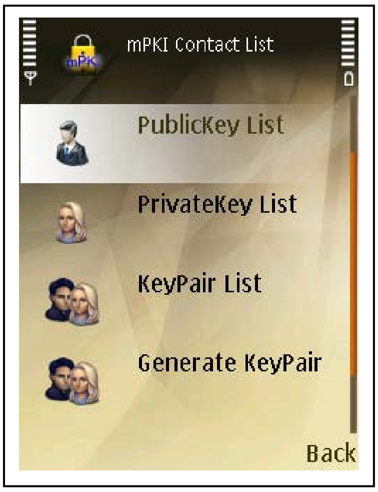


Fig. 1(b): MCA Interface

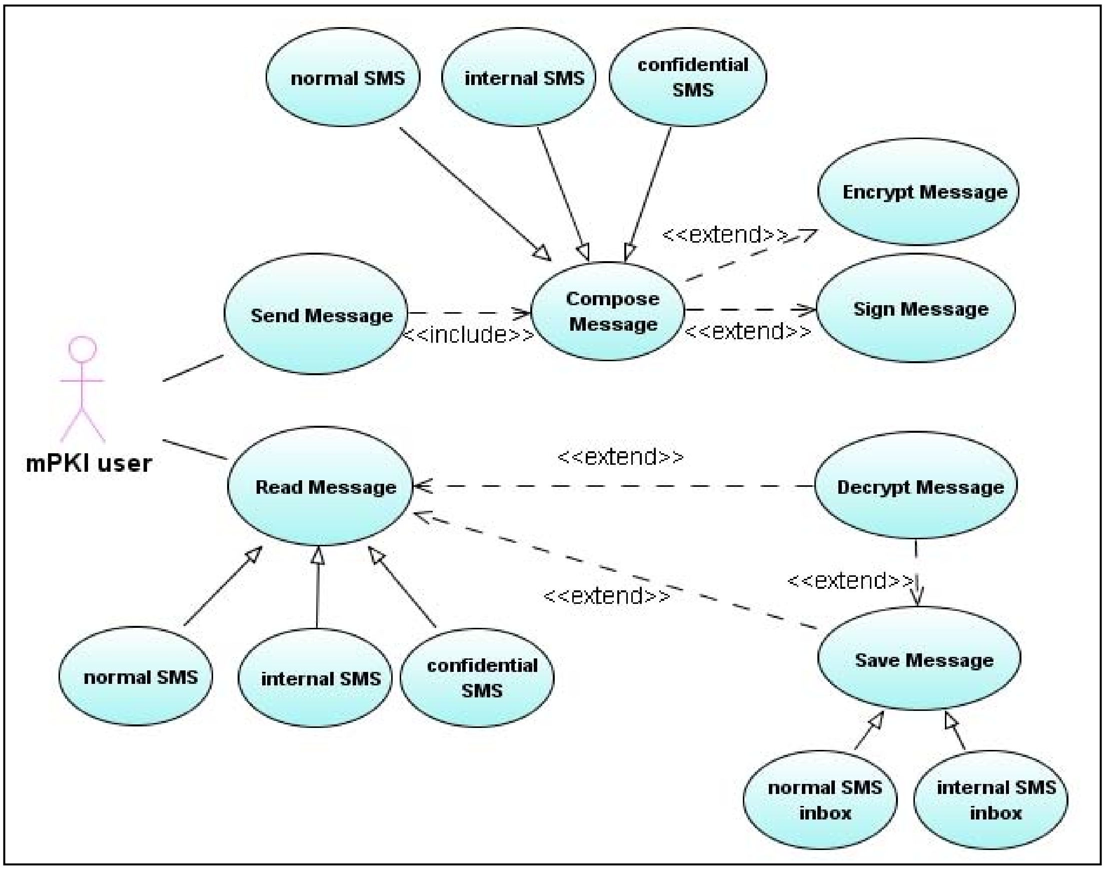
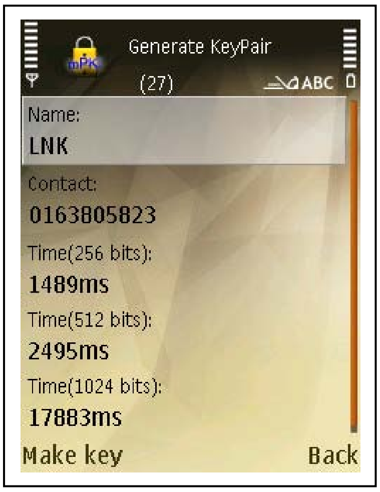


Fig.2: M-PKI's User Use Case Diagram

Generally, the public key is used to encrypt the message and the private key is needed to decrypt the message. These two keys are different. However, they are inter-related. If the message is encrypted by using public key of user *A*, it can only be decrypted by the private key of user *A* but not the private key of other user. In this situation, *M*–PKI's user is confident to use this message service in exchanging private and confidential information. Besides that, this category of messaging supports the non-repudiation concept in digital security to prevent forgery. The sender is required to sign the message with the private key. As a result, he or she cannot deny on sending that particular message.

3.1 Key generation and management

To ensure the performance in using *M*-PKI messaging services, analysis has been carried out on the key used. The key length is the essential element in deciding the security strength and system performance. In other words, the key pair with higher bit is more difficult to be broken compared to those in lower bit. On the other hand, longer time is needed to perform message encryption and signing.

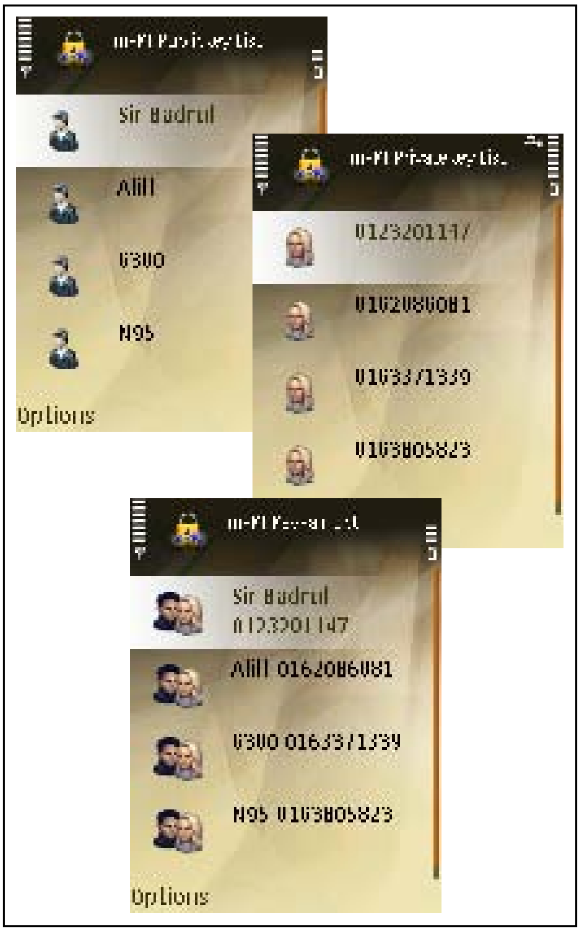


Name:
LNK
Contact:
0163805823
Time(256 bits):
1489ms
Time(512 bits):
2495ms
Time(1024 bits):
17883ms

Fig. 3: Testing On Various Key Lengths

Fig. 3 shows the testing result of RSA key pair generation with various key lengths on Nokia N95 handset. The comparison is made by measuring the time taken (in millisecond (ms)) to generate the different size of key pair (in bits). The time used on 256 and 512-bits is acceptable because it is less than three seconds whilst the 1024-bits consumes 18 seconds approximately. The bigger the key size, the longer the time of creation it takes. As a conclusion, the key size of 512-bits is selected based on the consideration on trade off between security and performance.

M CA is responsible for key pair generation and distribution. The generated key pair is stored in three separate record lists which are '*PublicKey List*', '*PrivateKey List*', and '*KeyPair List*'. Please refer to Fig. 4 for the illustration. These record lists are designed to ease the key distribution and management. Public key and private key are sent using *M*-PKI messaging services to the correspondent user. Both keys are stored automatically when reach at the phone.



Sir Badrul
Alili
6300
N95

0123201147
0162086081
0163371339
0163805823

Sir Badrul 0123201147
Alili 0162086081
6300 0163371339
N95 0163805823

Fig. 4: *M* CA's Public Key, Private Key and KeyPair List

3.2 Usability and performance of the application

The usability can be described as how user-friendly the system is. Besides that, usability also refers to the system learnability, efficiency, and user satisfaction. For example, if a system has a very complicated interface, it will decrease the user satisfaction due to bad experience on using it. Besides, if user fails to learn and use the system to perform task even training is provided, and then this also shows that the usability of the system is low.

The design of *M*-PKI is simple and user-friendly. The graphical interfaces have met the standard of user acceptance which are attractive, straight forward and all functions are visible to the user. The general flow of messaging is similar with the conventional messaging service. For the confidential SMS, all buttons are arranged in a sequence to help inexperience user interact with and use the system effectively.

$M-$ PKI's user interface design focuses on the message classification and protection. Fig. 5(a) is the interface of main screen. User can study about the $M-$ PKI's messaging services and offered security by clicking the "*About m-PKI*". The contact list, public key and private key list are grouped in *PKI Directory* as in Fig 5(b). The "*mPKI sms*" is designed to allow user to compose different types of message such as normal SMS, internal SMS and confidential SMS. All new messages excluding confidential SMS are stored in the inbox named as "*New Message*". This message buffer allows incoming message to be saved in the record list to prevent message lost.

Inbox is provided for normal SMS and internal SMS. Password protection is given to internal SMS only. This is to avoid unauthorised user from accessing the stored message if the phone is lost or shared. Besides, all messages from the category of confidential SMS are unable to be saved. In other words, all PKI message will has no trace on it because it is deleted right after the user exit the application. The application is designed in such a way so that the security of M-PKI is protected.

For addition, all messages, from internal and confidential, are encrypted when travel across the cellular network. This is to ensure the confidential information is safely protected from the middle-man attack and the unauthorised party such as administrator of message centre.

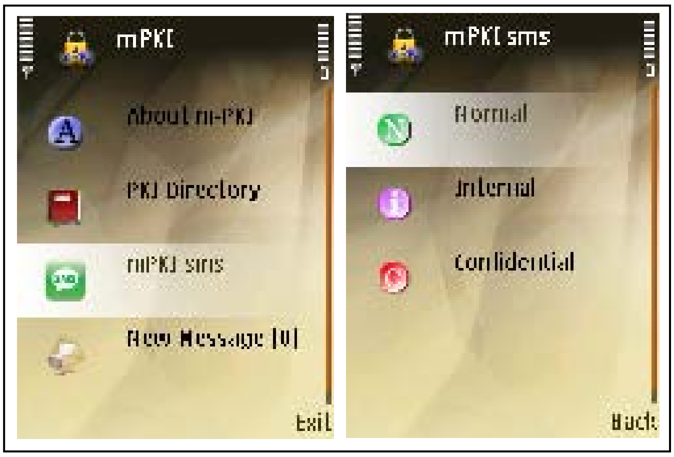


Fig. 5(a): $M-$ PKI's User Interface

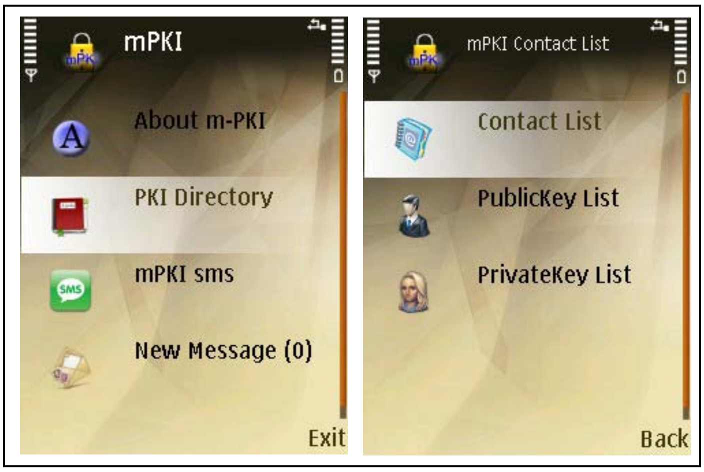
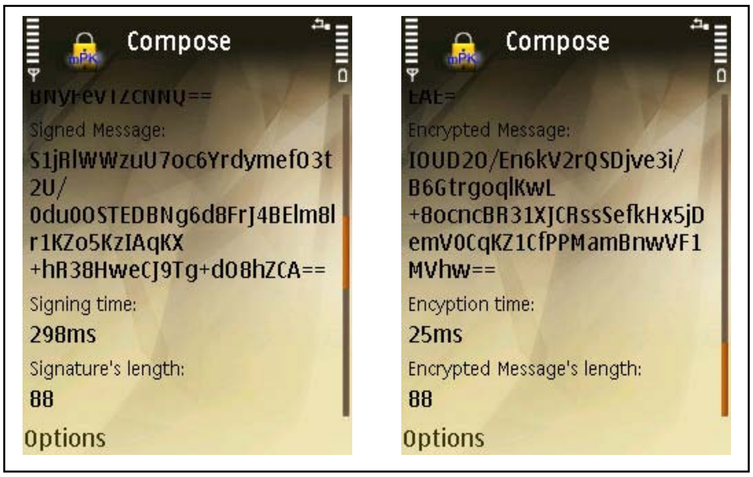


Fig. 5(b): PKI Directory

Testing on performance is the measurement of time in completing the system functionality. The testing focuses on the functionality of confidential SMS. The operation of message encryption, message decryption, signature generation and verification are involved. Fig. 6(a) displays the time used and the message length for the encryption and signing process in confidential SMS. The total time used on sending PKI message is 323 ms (*Encryption* + *Signing*) and the total message size is 176 bits (*Signature* + *Encryption*).

When the message reaches in the phone, the *decrypt screen* is appeared. The message consists of two parts which are encrypted message and sender's signature. The total size of confidential SMS exceeds the limit of single message (160 bits per message). It is reassembled when it reaches in the phone. The successful decryption displays the message in readable format as in Fig. 6(b). Time spent on performing PKI decryption is 237 ms and the verification takes 175 ms (total time was 412 ms). If signature is verified, a text is displayed to acknowledge the verification result. The testing result shows that the performance in sending or reading PKI message is very fast. It is due to the total time used which is less than one second. Fig. 6(c) demonstrates the fail decryption situation. The encrypted message is in unreadable mess and the signature is unverified with the wrong key is used. The testing successfully eliminates the concern on the middle-man attack when the message travels across the unsafe channel. The message confidentiality and impersonation are conserved.

M-PKI application can be run on all Java-enabled phones that support Mobile Information Device Profile (MIDP 2.0) including Symbian phone such as FOMA, Nokia, Samsung, Sony Ericson and Motorola. Since *M*-PKI is an application that offers mobile messaging service, the system reliability depends on the availability and adaptability of the current mobile network.



Compose

BNyFeVIZCNNQ==

Signed Message:

S1jRlWWzuU7oc6Yrdymef03t
2U/
0du0OSTEDBNg6d8FrJ4BElm8l
r1KZo5KzIAqKX
+hR38HweCJ9Tg+dO8hZCA==

Signing time:

298ms

Signature's length:

88

Options

Compose

EAE=

Encrypted Message:

IOUD2O/En6kV2rQSDjve3i/
B6GtrgoqlKwL
+8ocncBR31XJCRssSefkHx5jD
emV0CqKZ1CfPPMamBnwVF1
MVhw==

Encyption time:

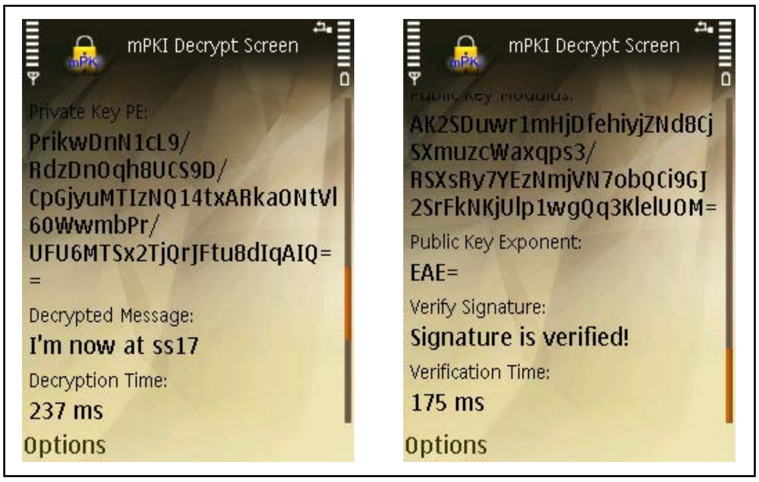
25ms

Encrypted Message's length:

88

Options

Fig. 6 (a): Performance On Sending Confidential SMS



mPKI Decrypt Screen

Private Key PE:

PrikwDnN1cL9/
RdzDn0qh8UCS9D/
CpGjyuMTIzNQ14txARkaONtVl
60WwmbPr/
UFU6MTSx2TjQrJFtu8dIqAIQ=
=

Decrypted Message:

I'm now at ss17

Decryption Time:

237 ms

Options

mPKI Decrypt Screen

Public Key Modulus:

AK2SDuwr1mHjDfehiyjZNd8Cj
SXmuzcWaxqps3/
RSXsRy7YEzNmjVN7obQCi9GJ
2SrFkNKjUlp1wgQq3KlelUOM=

Public Key Exponent:

EAE=

Verify Signature:

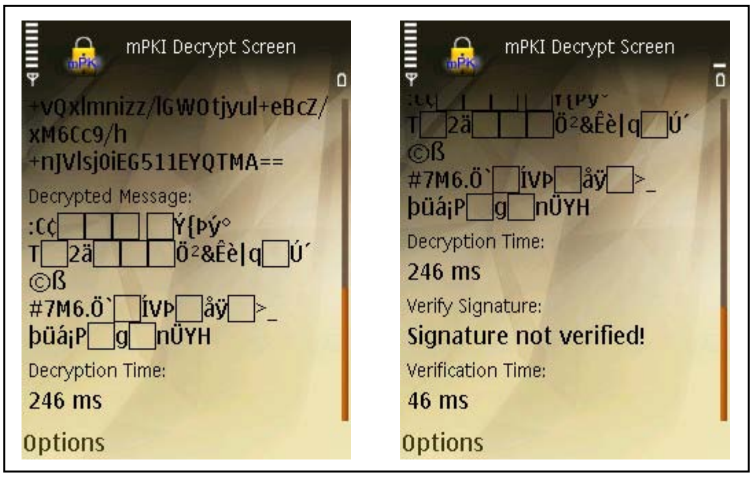
Signature is verified!

Verification Time:

175 ms

Options

Fig. 6(b): Performance On Successful Decryption



mPKI Decrypt Screen

+vQxlmnizz/lGWOtjyul+eBcZ/
xM6Cc9/h
+nJVlsj0iEG511EYQTMA==

Decrypted Message:

:C¢□□□□Ý{Þý°
T□2ä□□□Ö²&Êè|q□Ú´
©ß
#7M6.Ö`□ÍVÞ□åÿ□>_
þüá¡P□g□nÜYH

Decryption Time:

246 ms

Options

mPKI Decrypt Screen

T□2ä□□□Ö²&Êè|q□Ú´
©ß
#7M6.Ö`□ÍVÞ□åÿ□>_
þüá¡P□g□nÜYH

Decryption Time:

246 ms

Verify Signature:

Signature not verified!

Verification Time:

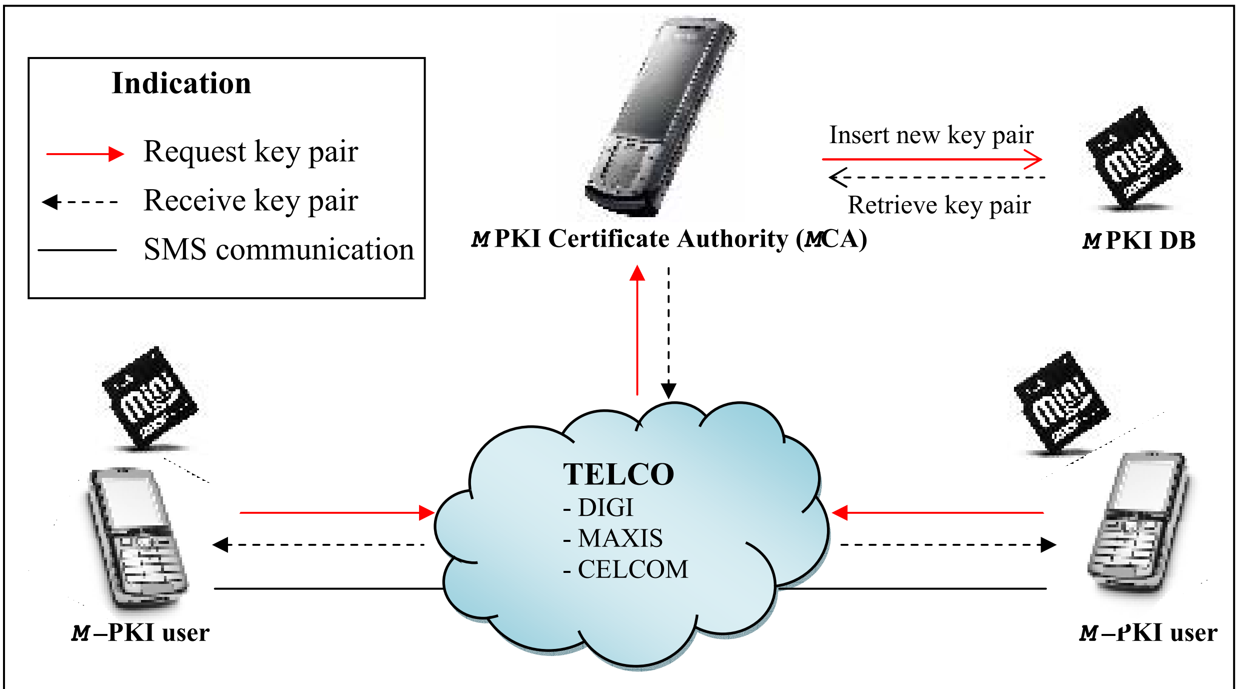
46 ms

Options

Fig. 6(c): Performance On Fail Decryption

Table 1: Testing On Malaysia's Mobile Network

Telecommunication Operator	Local Network	International Roaming
Celcom	✓	✓
Digi	✓	✓
Maxis	✓	✓



TELCO – Telecommunication Company

Fig. 7: Remote Storage For RSA Key Pair

Three major telecommunication network operators, which support different standard of mobile system in Malaysia, are listed in Table 1. Digi supports Global System for Mobile communication (GSM) network. Celcom and Maxis, on the other hand, provide Universal Mobile Telecommunications System (UMTS) network which combines third generation (3G) technology and GSM standard. Testing is focused on sending and receiving SMS via different local network. *M*-PKI's messaging service is also tested successfully by using international roaming.

4 Improvement on security

The internal SMS, which applies AES for message encryption, has a password-protected inbox. The saved SMS is safely guarded by this password. Besides, a contact list is provided for storing the symmetric key that used for the message encryption. On the other hand, confidential SMS consists of two key list which are public key and private key list. If the phone is lost, the user will lose those saved messages and the list of shared key, public key and private key as well. An alternative solution is suggested by having a removable storage. Please refer to Fig. 7 for the illustration.

The *M*CA is act as a mobile CA. All generated key pairs are stored in the Record Management System (RMS) and Secure Digital (SD) card. This removable storage is act as a backup for the RMS. Besides, it allows the application to have a mobile CA and eliminate the concern on the phone lost or theft. This concept is applied to the *M*-PKI's user as well. The inbox message and the entire *PKI*

Directory (contact, public key and private key list) are stored in the SD card. User can now free to switch to other phone with these SD card. The following is the sample coding to write file to the SD card [8].

```
public void createFile() {
  try {
    FileConnection filecon =
   (FileConnection)
   Connector.open("file:///SDCard/mynew
   file.txt");
     if(!filecon.exists()) {
       filecon.create();
     }
     filecon.close();
   } catch(IOException ioe) {
   }
}
```

However, the security in confidential SMS still can be improved. Access to the private key has to be restricted to the application owner only. If the application can offer a security control on accessing the private key, then the action of impersonating and message tampering could be avoided. Three different questions are prepared and the answers are set by the user. A question is asked randomly for each attempt on using the private key. The application becomes more secure to be used for private communication with this additional security control.

5 Conclusion

The reliability of the system refers to the availability of the system. A reliable system is always available in providing service. The reliability of *M*-PKI is high because the application does not crash during execution time. Furthermore, the probability of messaging service failure depends on the GSM network failure rate, which is very low. In addition, the chance of message lost is approximately to zero because the *new message inbox* stores the incoming message even the application is not started.

As a conclusion, implementation of PKI in mobile communication is the best solution for the subsequent decade. The demand for secure mobile encryption becomes increasingly important because too many applications have been built for mobile phone. Besides that, the PKI technology is easy to be understood and accepted by public. In addition, the implementation cost is economical and it is easy to be installed. However, the solution 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. However, it requires an 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.

The security strength of the encryption depends on the key size. The bigger the key size, the stronger the cipher text it produced. 2048-bit key length is suggested to be applied on data encryption in all application domains (either mobile or Internet) for the subsequent decade. The system performance may be affected but it can be solved by the technology since the processor power is getting powerful from day to day.

6 Future work

The significant use of mobile communication raises 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 into various wireless applications such as remote sensing and control on home appliances or hardware peripheral [9] on 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. In addition, medical services such as billing system, appointment booking and patient's record access [10] can be implemented via m-PKI.

Introducing biometric features such as voice and keystroke in encryption and decryption process will be the further study for this area. This feature ensures 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 is interesting and meaningful. The voice communication is the main attraction in mobile and internet applications. The repudiation in PKI helps in verifying the identity of target party. The recorded conversation can be used as legal evidence because all parties involved cannot deny the content and their participation on that conversation.

In future, perhaps new features or applications will be carried out for educational purpose. The verification for student identity during examination, academic assessment and personal information update can be done by using mobile PKI. Besides that, there is a demand to standardize the policy on key management. Building trust and maintaining trust relationship among different parties is difficult. The effort on applying PKI in various fields depends on government policy control.

Reference

[1]. eGov Strategy, "Mobile Data Association announces latest findings on UK mobile phone usage," July 31, 2008. [Online]. Available: http://www.publictechnology.net/print.php?sid=16852. [Accessed August 21, 2008].

[2] T. McCall and L. Goasduff, "Gartner Says Worldwide Mobile Phone Sales in First Quarter are Indicative of Another Strong Year in 2006," May 31, 2006. [Online]. Available: http://www.gartner.com/press_release/asset_152911_11.html. [Accessed August 21, 2008].

[3] J. Knudsen, *Java Cryptography*. O'Reilly, 1998, pp 6.

[4] National Security Agency And Central Security Service, "Fact Sheet NSA Suite B Cryptography," 10 January 2008. [Online]. Available from http://www.nsa.gov/ia/industry/crypto_suite_b.cfm?MenuID=10.2.7. [Accessed January 10, 2008].

[5] Federal Information Processing Standards Publication 197, *Announcing Advanced Encryption Standard (AES)*, 26 November 2001. [Online]. Available from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf . [Accessed 10 May 2008].

[6] GoodLink, "Encryption: AES versus Triple-DES," July 2, 2008. [Online]. Available from http://www.icommcorp.com/downloads/Comparison%20AES%20vs%203DES.pdf. [Accessed 2 July 2008].

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

[8] Q. Mahmoud, "Getting Started with the FileConnection APIs," December 2004. [Online]. Available: http://developers.sun.com/mobility/apis/articles/fileconnection/. [Accessed September 3, 2008].

[9]. 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.

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