Available online at www.elixirpublishers.com (Elixir International Journal)

Advanced Engineering Informatics

Elixir Adv. Engg. Info. 37 (2011) 3758-3763

ISSN: 2229-712X

The use of SET protocol in telemedicine

Abbas Toloie- Eshlaghy[1], Ebrahim Nazari Farrokhi[2] and Mohammad Nazari Farrokhi[3]

[1]Department of Industrial Management, Faculty of Management and Economics, Science and Research Branch, Islamic Azad University, Tehran, Iran

[2]Department of Information Technology Management, Faculty of Management and Economics, Science and Research Branch, Islamic Azad University, Tehran, Iran

[3]Department of Computer Science, Payam-e Noor University, Nour Abad Lorestan.

ARTICLE INFO

Article history:

Received: 6 June 2011;
Received in revised form:
17 July 2011;
Accepted: 27 July 2011;

Keywords

Secure electronic transaction (SET),
Telemedicine,
Electronic commerce,
Cryptography,
Digital signature,
Technology,
Hash function.

ABSTRACT

Although electronic commerce has a lot of advantages it suffers from technological and non-technological limitations as well which have hindered its growth and acceptation. The imagination of insecurity and the lack of internationally accepted standards for quality, security and reliability are among the most important technological and non-technological obstacles facing electronic commerce. The insecure imagination of this technology has led to carrying out financial transactions by customers using traditional methods. Now, the question is raised that how the security of electronic financial transactions can be guaranteed for customers? Secure electronic transaction (SET) is one of the most important security protocols and guarantees the security of transactions of any kind. The present article explains the use of this protocol and the method of applying it in Telemedicine. Also, advantages and disadvantages of using SET will be discussed.

ntroduction

Electronic commerce programs in the early 70s started with innovations such as electronic transaction of money. Meanwhile, such programs were limited to large organizations and a number of daring small businesses. Later on, electronic information transaction was invented which made electronic processing of ordinary transactions possible and expanded electronic commerce to all fields of industry (Turban, 2006). Electronic commerce transactions can be carried out among different groups. One of the transactions is carried out among people with each other. In this case, a person sells products or services to other ones (consumer-to-consumer). The term customer-to-customer is also used in this case (Turban, 2006). Since Internet was commercialized and websites were emerged in the early 90s, electronic commerce programs have rapidly developed. In 2000, electronic commerce activities faced a crisis which lasted for nearly three years. This issue caused hundreds of internet companies to be shut down. Since 2003, electronic commerce has continued growing. Nowadays, most of large and medium scale organizations and a majority of small scale companies utilize some methods of electronic commerce (Turban, 2006).

Electronic processes have gained a very special place after the expansion of information technology and internet around the world. In electronic processes, the optimum use of internet and speeding up is followed as a goal. Today, many institutions spend much time on offering information through the worldwide web or internet. The main reasons for using internet are:

- Promoting services across the globe
- Reducing operational costs effectively among elements of a meeting
- Increasing revenues through new customers and channels along with new products and services
- Winning customer satisfaction
- Offering online services
- Speeding up service rendering and employing specialized manpower who are in another place

Limitations of electronic commerce

Although electronic commerce has a lot of advantages it suffers from technological and non-technological limitations as well which have hindered its growth and acceptation. The limitations and obstacles are as follow:

- Technological limitations of electronic commerce:

Passing time has reduced, or removed, limitations, especially technological limitations. In addition, proper planning can minimize negative effects of some of them. These limitations include:

- Lack of globally accepted standards for quality, security and reliability
- Insufficient remote communication bandwidth
- Software development tools which are to be developed
- Problems of integrating electronic commerce and internet programs with some existing programs and websites
- The need to special web servers in addition to network servers
- Expensive or improper access to internet for many of online users

- Non-technological limitations of electronic commerce:

- Insecurity imagination and expensive electronic commerce
- Insufficient governmental and international laws and industrial standards
- Lack of comprehensive methods to assess benefits and justify electronic commerce
- Lack of public trust to non-paper and remote transactions (Turban, 2006).

Tele:
E-mail addresses: toloie@gmail.com, e60_itmgtn@yahoo.com

Internet is widely used in medical sciences. Precious experience of a specialist, which can save lives of people, may not be available to everyone due to physical limitations. Electronic interaction can be of special advantages and capabilities in this regard. However, the weak understanding of people from network security has hindered rapid growth of this issue, because most of trade dealings are carried out using credit cards, users are worried about their personal information to be disclosed. Hackers and some fake credit cards have escalated the worry. This issue has even affected the use of medical science form this technology, so that it has caused many experienced doctors not to offer services to patients due to misconduct of some other doctors. Perhaps they think that their fees may not be paid via internet. Moreover, patients may think how they can prove a wrong decision which is taken by a doctor during diagnosis and the doctor can not reject the decision. Using the SET protocol, a user can become assured of a secure system to use his/her credit card. In addition, any kind of decision making and information exchange among members of a meeting can be pursued in the future by the members. SET is a set of security protocols which enable users to apply their confidential information securely on their credit cards in the worldwide internet.

SET exchanges messages and information among users and server using cryptography, so that if hackers access to the encrypted information, they will never be able to decrypt the information. In addition to confidentiality, SET maintains genuineness and integration of messages. Considering sensitivities in medical diagnosis the protocol secures genuineness of the sent message.

Using this protocol even the institution in which the user has applied his/her credit card (such as a hospital) will not be able to decrypt the user's credit card number (this is done in line with maintaining security of the credit card's specifications). Both the hospital and the doctor will become assured of genuine identity of each other using this protocol. From among other advantages of SET is that the dealing sides can not deny the exchanged information. This article has discussed cryptographies, identity confirmation of the parties, digital signature, digital certificate, and the method of using the SET protocol in medical sciences.

SET technology

- Advantages of using SET protocol

The SET protocol has three main advantages which have made it more reliable than other methods. The three advantages are:

- Confidentiality: This is done using cryptography which makes reading messages by others impossible.
- Genuineness: Using message abstract and signature confirmation they assure that messages are transferred without any change
- Confirmation using digital signature: This assures that claims of the dealing parties are provable and their acts are undeniable.

SET services

SET offers three services:

▪ Providing a secure telecommunication channel among all parties involving in a transaction

▪ Creating confidence using digital certificate X509V3

▪ Guaranteeing limits because information should be accessible by the parties in a transaction at each time and each place which is necessary

- SET components

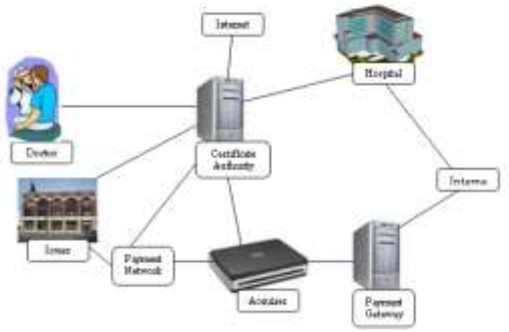

Figure (1): Different elements of a SET system

○ Cardholder: The cardholder in an electronic environment is referred to customers and legal persons who are in mutual relation with the seller via personal computers connected to internet. A credit card holder is the holder of a payment card like Master Card, Visa, etc. which have been issued by a reference. In this article, it is the patient.

○ Issuer: It is a financial institution, such as a bank, which issues cards for users and is responsible for paying users against their purchases.

○ Acquirer: It is a financial institution which opens accounts for users and includes permissions for payments and processing payment cards. In addition to controlling over active accounts, the acquirer presides over drawing out money from cards over the allowed amount. It is also responsible for transferring sums to accounts of other users electronically.

○ Payment gateway: It is an operating function which is run by the acquirer, so that it processes financial messages of users. In fact, it is an intermediate between the SET and financial networks of the existing card bank which defines financial authorities and responsibilities. By the time the payment gateway is connected via the network to the financial processing system of the acquirer, users exchange the SET messages using the payment gateway on the internet.

○ Certification authority (CA): This is a centre which issues X509V3 public certificate for users and payment gateways. Success and result of the SET is dependent upon existence of a CA infrastructure. CA is hieratically applied, so that there is no need to issue permissions for users directly by the root.

Cryptography in the SET protocol

The SET basically uses cryptography toward its objectives, so cryptography is briefly described:

- Issues related to cryptography: Publicly speaking, cryptography systems are divided into symmetrical and asymmetrical cryptography systems.
- Symmetrical cryptography system: The main condition for the existence of such system is based on a secure channel because a private key exists in this system which can reveal the whole information in the system if it is disclosed. This key is sent from cryptographer to decoder through the channel. In other words, the keys for cryptography and decoding are both the same. In fact, having one the other can be calculated easily. So, the existence of the secure channel seems to be necessary. The two distinguished cryptography algorithms are information encryption standard (DES) and advanced encryption standard (AES). In the SET protocol, the DES symmetrical encryption is used.
- Asymmetrical cryptography system (public key): In systems with public keys it is considered that there is no secure channel. Of course, no one can imagine a fully secure channel. Therefore, in this kind of cryptography, it is assumed that there is no secure

channel and the hacker is seeing the message, but the hacker has not understood the idea and meaning of the message and can not obtain any useful information from seeing the message. In this system two couples of key exist in practice:

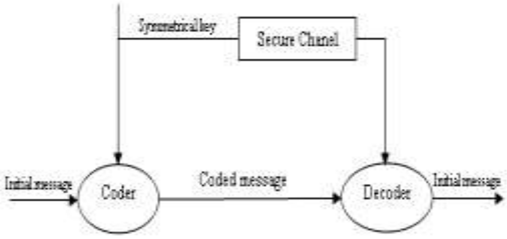

Figure (2): A view of Symmetrical cryptography system

o **Public key:** Each person can use the key to encrypt a message and send it.

o **Private Key:** Using the private key, the receiver can decrypt every encrypted message and only the private key can decrypt an encrypted message. Even the person who has encrypted the message will not be able to decrypt the message without having the private key. In other words, the special feature of the private key is that even holding the public key one can not gain any information regarding the private key. Rivest, Shamir and Adleman(RSA) and RABIN are among encryptions using the public key.

For example, the user 1 and the user 2 want to communicate using asymmetrical encryption method. At first, the two sides should agree on a specific encryption algorithm such as RSA. Then, for instance, the user 1 should have a public key and a private key (generating such keys requires conditions which have been discussed in the encryption subject). The user 1 sends his/her public key for the user 2 through an insecure channel. In other words, the public key is accessible to everyone (which is not important), but the user 1, which holds the private key, is the only person who can decrypt the encrypted messages. Of course, each person who holds the public key can send the user an encrypted message. The Rivest, Shamir and Adleman (RSA) is used in the SET protocol.

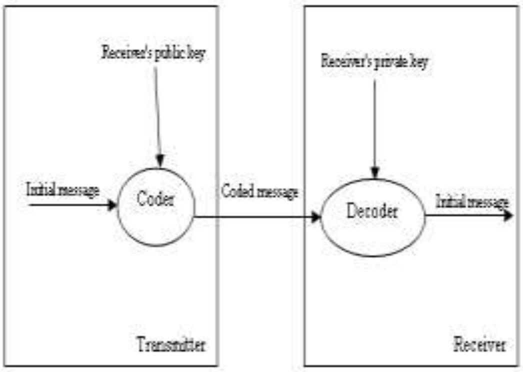

Figure (3): A view of the public key system

DES cryptography: The DES has been designed using a 1024-bit code which has turned it into one of the most reliable asymmetrical cryptography methods or the private key. To decrypt such a code, one hundred computers, each running ten millions of jobs per second, should work for over 2,800,000,000,000 years in order to decode the message and the same amount of time is needed for the next message.

RSA cryptography: In this system, two large prime numbers, such as *p* and *q*, are selected, so that $n = pq$, and then a set of messages and codes are considered as members of Z_n. Then,calculate $\varphi(n) = (p-1)(q-1)$ and select $1 < b < \varphi(n)$ So that $(b, \varphi(n)) = 1$.

Then, based on the inverse member theory for *b*, exists in $\varphi(n)$. If the inverse member is calculated using the Euclidean algorithm and call it a, then (n,b) is announced as the public key and $(p,q,\varphi(n),a)$ is kept as the private key. Now, the method of encrypting is applied as follows:

$e_k(x) \equiv x^b \equiv c \bmod(\mathrm{n})$ (1)

And the decoding message is applied as follows:

$d_k(c) = c^a \equiv x \bmod(\mathrm{n})$ (2)

So, *a* remain as the private key for confidential cryptography and *b* is announced as the public key.

Hash function and its specifications: The hash function is a function that receives each length if input and returns a fixed length to us.

Such function is called the storage hash function, which is a public function. For example, the hash function gets each length from $\{0, 1\}^*$ and turns it into $\{0, 1\}^{160}$. So, the hash function is not a one-to-one function. It should be noted that the hash function should be considered in a way that it does not provide the situation for the enemy's attack. From among the situations, it can be referred to the following point.

h(x) should be so that finding a *x'* be impossible in the following way:

$x \neq x' \Rightarrow \mathrm{h(x')} \neq \mathrm{h(x)}$ (3)

We know in the case of using the hash function, signature will be in the following form:

$y = sig_k(h(x))$ (4)

Now, if the abovementioned function is applied, the forger will give (x', y) to the receiver. The receiver will decrypt the signature using the public key and reaches *h*(x). In this time, the hash function is applied to *x'* and since $h(x) = h(x')$, the forged signature is confirmed.

Digital signature

The first thing to consider is that digital signatures are different from ordinary signatures in the following points:

- In a digital signature, the message and the signature are completely independent from each other. But, in an ordinary signature, the signature is a part of the message and is not separate from the message.
- Forging an ordinary signature is very easy, but forging a digital signature is very difficult, or in other words, it is theoretically impossible.
- Confirming an ordinary signature is not easy and, of course, not common. But, a digital signature can be easily confirmed by everyone.

Each digital signature has two stages: Signing and confirming the signature. Each signature has two elements: the private key and the public key. Basically, only the owner of the private key would be the owner of the signature, who can carry out signing. But, the signing regulation is that all can confirm the signature. So, the public key will be available to everyone in order to confirm the signature. One of the most important signing algorithms is the RSA algorithm which is briefly described as follows:

In this system, x is the real message, $n = pq$, in which n is announced publicly, but *p* and *q* are private (in other words, if n is separable, forging the signature will be very easy (the issue was discussed in the cryptography section). $ab \equiv 1(\bmod \phi(n))$, in which *a* is the private key and *b* is the public key. Signing is carried out as follows:

$$y \equiv x^a(\bmod(n)) \qquad (5)$$

So is sent in the form of (x, y), i.e. the signature along with the message. In the destination, the receiver receives (x, y) and estimates *b*, *y*, and y^b having the public key. If it was equal to x, the signature will be confirmed. Otherwise, the signature will not be valid by the receiver and can not be accepted.

Stages of carrying out the SET scenario

- Users open accounts: Users receive a credit card such as Visa or Master card from a bank which can support electronic payment and the SET, as well.
- Users receive digital confirmation. After investigating each person's identity, users receive X509V3 digital confirmation which can be validated by the bank. This certification specifies the user's RSA public key as well as the card's expiry date. Also, it establishes a guaranteed link by the bank between the user's keys and the credit card. Institutions have their own certificates, as well. An institution accepts a certain kind of card and should have two certificates for its public key, one for the signed messages and the other for exchanging and replacing the key. Also, a copy of the certificate of the payment gateway's public key is needed.
- The hospital's server starts interaction with the doctor: This is a process in which the patient starts required experiments in the hospital and then results of the experiments are sent to the online doctor.
- The doctor is revised: The doctor sends a copy of his certificate to the hospital's server because the hospital should affirm the doctor's identity.
- Medical information is sent: The server sends financial and medical information along with its certificate to the doctor for assuring the doctor of the hospital's true identity. The medical information includes the carried out experiments related to the patient, and the payment information includes details of the credit card. The payment information is decoded to the extent that they can not be read by the doctor. The hospital's certificate enables the doctor to identify the hospital.
- The doctor request the payment permission: The doctor sends the payment information to the payment gateway and requests to be certified that whether the patient's credit card is valid for the purchase. If validated by the payment gateway, the process is continued.
- The doctor sends his diagnosis to the server.
- The doctor requests costs: This request is sent to the payment gateway which runs all financial processes.

Dual or double signature

The aim of dual signature is to link two messages which have sent to two different receivers. In this case, the server sends order information (OI) to the doctor and the payment information (PI) to the bank, as well.

It is not obligatory for the doctor to know any information on the number of the patient's credit card and, vice versa, the bank does not need to have any medical information. The server causes more security for maintaining these two separate items observing limits. Anyway, the two items should be so linked that to be used to remove this problem. The link is necessary for the two sides to prove that the payment is for this service and not for other services.

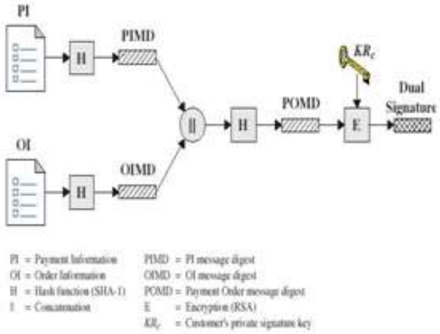

Figure (4): The method of using dual signature

Structure of a dual signature: The server applies the hash function on OI and PI. These two hashes are connected to each other and finally the server encrypts the resulted function using its private key signature.

$$DS = E_{KR_c}[h(h(PI) \| h(OI))] \ (6)$$

KR_c is the customer's private signature key. Now, the server is the owner of the OI dual signature and the PI message digest (PIMD). The doctor also holds the server's public key which has been received from the server's certificate certificate. So, the doctor can compare the two following quantities shown below:

$$h(PIMD \| h(OI)) \qquad (7)$$

$$d_{KU_c}[DS] \qquad (8)$$

KU_c is the server's public signature key.

If the two abovementioned amounts are equal, the doctor identifies the signature. Similarly, if the bank can do the below comparison and the two equations are the same, the bank will certify the patient's signature.

$$h(h(PI) \| OIMD) \qquad (9)$$

$$d_{KU_c}[DS] \qquad (10)$$

In summary, the doctor receives OI and identifies the signature. The bank receives PI and identifies the signature. Also, the hospital's server relates OI and PI and can prove the relation.

Details of a transaction

In order to make complexity of SET perceivable, let take a look at one of the common transactions and study it. Before the transaction starts, the card holder should finish searching, selecting and ordering as well as required experiments on the patient. Then, internet transaction will start. The transaction request includes 4 messages:

- Start request, from the hospital's server to the doctor
- Start response, from the doctor to the server
- Exchange request, from the server to the doctor
- Exchange response, from the doctor to the server

To send SET messages to the doctor, the server should hold a copy of the doctor's certificate and the payment gateway, as well. In the start request message, the server request for certificate and sends it to the doctor. The message carries the credit card's trademark which is used by the patient. The message also includes the ID attributed to both request and response. The doctor generates a response and shows it using the private key. The response includes an ID exchange for the transaction. In addition, for the specified response, the response start message includes the doctor's and the payment gateway's certificates. The server checks the doctor's and the payment gateway's certificates as well as the CA signature related to it. Then it builds the order information (OI) and the payment information (PI). The ID attributed to the doctor has been placed both in the OI and in the PI. Apparently, OI specify medical data. Then, the server prepares the interaction request message server.

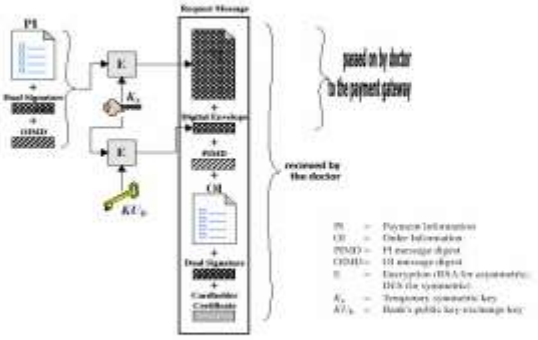

Figure (5): Details of a purchase request

The server sends a interaction request: To this end, the server generates a decoded DES key, which is known as Session Key. The message includes the following information:

- Payment information: This information is sent by the doctor to the payment gateway and includes PI and a dual signature. Both are decoded in a moment by the Session Key.
- Finally, the Session Key is encrypted with the payment gateway's public key and is added to the message, so that only the payment gateway is able to decode the message and read the Session Key. So, only the payment gateway is able to receive and recover PI.
- Medical information: This information is required by the doctor and includes OI and PI. The doctor uses dual signature for identifying validation of OI.
- Validating credit cardholder: It includes the patient's public key which is required by the seller and the payment gateway. When the seller receives a request for interaction, the following activities are done:

○ Specifies the credit card certificate using its CA signature.

○ It specifies the dual signature used in the server's public signature key. This issue guarantees that the order has not been manipulated and it has been specified using the server's private signature key.

○ Information is processed and the payment information is sent to the payment gateway for being authorized.

○ The doctor's diagnostic results are sent to the server.

○ The interaction response message includes a blocked response which covers the doctor's diagnostic results and returns the correspondent exchange number.

○ This block is specified by the doctor using the private signature key. The block and its related signature are sent to the server along with the doctor's signature certificate.

Unresolved problems and difficulties of SET

Although SET has the potential to establish security on the internet and this way it guarantees reliability of online communications, but it still suffers from some unresolved problems.

The important issue is the link among programs that have been developed by different software developers. By the time the problem is resolved, the SET standard can not be spoken of. Another problem is the system's integration which exists specifically in sites which want to launch the SET technology on their current systems. Now, we will study the two problems in detail:

- Mutual relation possibility

Compatibility among different SET software products is necessary. If this protocol wants to be used for a long time as an open protocol, users should have the possibility to select software from among a variety of software products from different companies. This is of importance that they work together without any defect. This issue has not been realized to date. In fact, a small number of produced software products are compatible with each other. If it is realized, its standard will be undoubtedly very extensive.

- Merging systems

Besides the issue of mutual relation, another problem exists in relation with the SET protocol. To answer the question of to what extent the SET protocol and e-business models which are used has been merged? It is better to take a look at a research study. But, prior to that, it should be mentioned that the study covers the merger of the SET-based systems and systems which are used by sellers to build web stores. It depends mostly on factors such as the existing methods for accounting, data exchange and invoice writing. Ibis was the founder of projects in which it was seen during preliminary development of SET worldwide that security systems have major problems. In the preliminary testing of the project in Sweden in which 30 companies were participated, the problem was shown clearly. Technical problems of the Swedish project were not only due to the merger, but the merger caused many problems.

In addition to the two abovementioned problems, low speed and expensiveness of SET were other important issues, so that a transaction requires six digital signatures, nine RSA cryptography and decoding operations, four DES cryptography and decoding operations, and four X509 digital certificates validation phases, all of which cause lowering speed as well as appropriate hardware and software by the transaction sides. The low speed hinders it from being used in some medical cases which need high speed of below a second.

Conclusion

It is understood from the text that SET has a number of problems and deficits. Now the question raises that will SET be accepted as a standard for e-business? Some believe that SET is very expensive and complicated, while some others say SET is just the thing e-business requires and it is attractive and reliable for all purposes.

The fact is that SET is supported by very powerful entities (such as banks and credit card companies) which benefit from its promotion and it is an undeniable chance for them. Visa and Master Card have greatly invested in it. At present, all transactions via internet are conducted with a high degree of risk. Perhaps offering low cost services can be a suitable incentive to persuade companies, institutions and users toward applying SET despite all its deficits, because it can guarantee the security of electronic transactions.

References

D. Bleichenbacher, B. Kaliski and J. Staddon. Recent Results on PKCS #1(1999). RSA Encryption Standard. RSA Laboratories' Bulletin. No. 7.

D. Chaum(1983).Blind signatures for untraceable payments. Advances in Cryptology-CRYPTO'82. pp. 199-203.

D. COPPERSMITH, M. FRANKLIN, J. PATARIN AND M. REITER. LOW-EXPONENT RSA WITH RELATED MESSAGES. IN U. MAURER(1996). ADVANCES IN CRYPTOLOGY – EURO CRYPT '96, VOLUME 1070 OF LECTURE NOTES IN COMPUTER SCIENCE, PP. 1 – 9. SPRINGER VERLAG.

Elsayed Mohammed, A. E. Emarah and Kh. El-Shennawy(2000). A Blind Signature Scheme Based On ElGamal Signature. EUROCOMM 2000, Information Systems for Enhanced Public Safety and Security IEEE/AFCEA, pp.51.

J.-S. CORON, M. JOYE, D. NACCACHE AND P. PAILLIER(2000). NEW ATTACKS ON PKCS #1 V1.5 ENCRYPTION. IN B. PRENEEL, EDITOR, ADVANCES IN CRYPTOLOGY – EURO CRYPT 2000, VOLUME 1807 OF LECTURE NOTES IN COMPUTER SCIENCE, PP. 369 – 379. SPRINGER VERLAG.

Kevin Lam, David Leblanc, and Ben Smith (2004).ASSESING NETWORK SECURITY", ppt 155-165.

M. BELL ARE, A. DESAI, D. POINT CHEVAL AND P. ROGAWAY(1998). RELATIONS AMONG NOTIONS OF SECURITY FOR PUBLIC-KEY ENCRYPTION SCHEMES. IN H. KRAWCZYK, EDITOR, ADVANCES IN CRYPTOLOGY – CRYPTO '98, VOLUME 1462 OF LECTURE NOTES IN COMPUTER SCIENCE, PP. 26 – 45. SPRINGER VERLAG.

Wikipedia(2006). The Free Encyclopedia. VeriSign. Retrieved on from: http://en.wikipedia.org/wiki/VeriSign.