J Med Syst (2011) 35:735–742
DOI 10.1007/s10916-009-9414-2

ORIGINAL PAPER

Electronic Medical Archives: A Different Approach to Applying Re-signing Mechanisms to Digital Signatures

Tzer-Long Chen · Frank Y. S. Lin

Received: 16 September 2009 / Accepted: 30 November 2009 / Published online: 22 December 2009

Abstract Electronic medical records can be defined as a digital format of the traditionally paper-based anamneses, which contains the history of a patient such as his somewhat illness, current health problems, and his chronic treatments. An electronic anamnesis is meant to make the patient's health information more conveniently accessible and transferable between different medical institutions and also easier to be kept quite a long time. Because of such transferability and accessibility of electronic anamneses, we can use less resource than before on storing the patients' medical information. This also means that medical care providers could save more funds on record-keeping and access a patient's medical background directly since shown on the computer screen more quickly and easily. Overall, the service quality has seemingly improved greatly. However, the usage of electronic anamneses involves in some concerned issues such as its related law declaration, and the security of the patient's confidential information. Because of these concerns, a secure medical networking scheme is taking into consideration. Nowadays, the administrators at the medical institutions are facing more challenges on monitoring computers and network systems, because of dramatic advances in this field. For instance, a trusted third party is authorized to access some medical records for a certain period of time. In regard to the security purpose, all the electronic medical records are embedded with both of the public-key infrastructure (PKI) cryptography and the digital signature technique so as to ensure the records well-protected. Since the signatures will be invalid due to the revocation or time expiration, the security of records under this premise would turn into vulnerable. Hence, we propose a re-signing scheme, whose purpose is to make a going-expired digital signature been resigned in time, in keeping with the premise of not conflicting with the laws, morals, and privacy while maintaining the security of the electronic medical records.

Keywords Electronic anamnesis · Public key infrastructure · Re-signing · Digital signature · Electronic signature law

T.-L. Chen (✉) · F. Y. S. Lin
Department of Information Management,
National Taiwan University,
Taipei, Taiwan
e-mail: d97725005@ntu.edu.tw

F. Y. S. Lin
e-mail: yslin@im.ntu.edu.tw

Introduction

Health information management is evolving as the most of medical care providers are thinking and focusing on how to grow the business from a regional joint cooperation to a globally integrated medical network platform [1]. How can this be achieved? The network and information system programs will do and help to achieve this goal. Let's imagine what the future of your local hospital would be. Just pretend you are walking into a hospital 5 years from now. What would be the things that you probably don't have to do; especially, if you are a transferred patient from one medical institution to another? The answer is that you don't have to rewrite all the paperwork associated with your health information and you don't have to request your medical documents from the previous institutions. That means you just go to the hospital you want to and don't care about any information you need to carry. Ideally, all medical care providers in the future are going to build a digitalized and sharing information network so as to keep

patients' anamneses more integral and more freely transferred from one to another. Electronic anamnesis is the key to achieve this goal. However, some concerns may rise when electronic anamnesis is used in medical informatics. Is this safe to transfer the patient's information through the network? Needless to say, if a secure scheme is well constructed, all the patients' information will be transferred on the network securely. The reason why we choose the electronic anamnesis as a starting point is that we believe the health care management must have got a headache on keeping those ever-growing archives. But the progress on solving these security concerns is not much touched by the researchers.

Traditionally, patient's anamneses are kept in paper formats. Nevertheless, there are two disadvantages of using paper-based anamneses. Firstly, paper can be easily damaged or lost when time passed by. The collection of the archives usually goes more and more such that the patients' information would become very difficult to look after or sort out. Imagine stacks of document papers, damaged by all sort of unforeseen cases such as fire, flood, insects, and humidity. If the archives were damaged, the doctors would face great difficulty on examining their patients, because they can't make a right prescription or treatment without knowing what kind of illness a patient may have experienced before. At the end, the patient has to be reexamined. Thus, how to improve the storability of these archives is a way to go. Secondly, the doctor would feel troublesome to trace the health history of a patient; especially, he is transferred from another hospital with their non-standardized paper-based documents. Therefore, the electronic anamneses are suggested to use so as to avoid the risk and inconvenience caused by the paper-based anamnesis.

Once the medical archives are digitalized, the electronic anamneses are capable of being transferred through the Internet when a patient's document is requested. However, the patient's document has to be transmitted under a safe public network environment or be stored at an untampered medium, such as compact disc and etc. If not, the documents could be duplicated, faked, and tampered by an unauthorized party. Once the information is tampered or stolen, it will seriously affect the confidentiality of the patient's personal information. Moreover, the level of security requirements is likely to increase over time while the computer technology continues advancing.

Our paper is to propose a re-signing scheme that involves in digital signature and time stamp techniques so as to improve the integrity and storability of electronic anamneses. A re-signable time stamp is applied to the electronic anamnesis embedded with a digital signature when the anamnesis is transmitted through the Internet or storable media.

Method

Before the electronic anamneses are built and used, some issues must be considered [2, 3]. The first issue is of how to avoid the risk of the electronic medical records facing the possible security breach during the transmission over the Internet and still keeping them been effectively accessed. We use the public-key infrastructure (PKI) security scheme as our fundamental cryptosystem to solve the problem. Under this system design, a digital signature is inserted into each electronic medical record as soon as it is created. Having digital signatures on those records can prevent them from tampering so as to ensure the integrity of electronic anamneses. However, digital signature is not long-lived though. It would expire after a certain period of time; thus, a re-signable time stamp technique should be applied to enhance the functionality of the digital signature.

Digital signatures

Digital signatures are valid to be used in private communication on the basis of an agreement among all related parties. All specific digital contents are capable of being encrypted and decrypted to ensure their integrity and non-repudiation. The concept of digital signatures originally coming from cryptography is a way to encrypt or decrypt senders' text messages by applying a hash function to keep the messages secure when transmitted.

A one-way hash function is a mathematical algorithm, which takes any length of a text message as input and gives an output in a specific length. Its main function keeps the encrypted output impossible to be derived by a third party [5]. Based on one-way hash functions, a digital signature scheme can be done as follows. A sender firstly uses a one-way hash function to convert an electronic medical record into a text message in a specific length, which is called the message digest [4]. Then, the sender will use his private key to sign on the message digest. A digital signature is generated. For a designated recipient, he can use the sender's public key on another one-way hash function to decrypt the received digest. The main purpose in the paper is to present a conceptual and helpful strategy to current medical systems. We also introduce some popular hash functions, such as SHA-1, RIPEMD-160 and MD5, able to be chosen to do encryption or decryption. Instead of choosing other more complicated algorithms to establish a cryptosystem, a hashing function makes the output messages with fixed length and guarantees the security of the cryptosystem because of its one-way property, which also lets the verification afterwards more convenient. However, if you are looking for a complicated one, we recommend Elliptic Curve Cryptosystem (ECC). ECC is shown to provide much greater efficiency with order of magnitude

roughly 10 times than the other public-key cryptosystems because of its property of shorter key length and lower computation. Therefore, that will be helpful in performance [6, 7].

Usually, a cryptosystem is used to protect the data transmitting through the Internet from tampering by an illegal third party. For instance, a document is encrypted by a sender's private key before sent out. Thus, the encrypted document only can be derived by a legal receiver who got the sender's public key. It is impossible for an illegal party to get the contents of the document decrypted, except the sender's private key is obtained and used to decrypt the message. In brief, the sender holds a private key and the receiver has the right to use the sender's public key, which is defined by both parties under a mutual agreement. When a receiver gets a document along with its digital signature, he has to use the sender's public key to further verify the validity of the document. Obviously, this method can help to ensure the security of data transmission. How a digital signature works under a Public Key cryptosystem is shown as in Fig. 1. If the sender must sign a message to the recipient, the sender uses its own private key through calculation of the hash function D to gets S_i as the signature of the message. When the recipient receives the message and the signature S_i, it can use the sender's public key to verify the signature for the message through the hash function E. If the calculated message is not the same as the message itself, it is possible to get an illegal document because of being tampered. On the contrary, it is the valid document that the recipient wants. As stated above, a hashing function makes the output messages with fixed length and guarantees the security of the cryptosystem because of its one-way property, which also lets the verification afterwards more convenient. Therefore, using hash functions to do the integrity verification is quite secure.

Public-key cryptosystems

The concept of public-key cryptosystems was first proposed by Diffie and Hellman in 1976. They opened a new direction on cryptography development. Since then, many researchers started to propose various types of public key cryptosystems [8, 9].

Public-key cryptography [10] is a kind of asymmetrical encryption technique. Each party in such cryptosystem holds two keys; one is the public key used to encrypt a datum and the other is the private key used to decrypt. Presumably, the sender uses the recipient's public key to encrypt the message and the recipient uses his private key to decrypt the received message. Even although this cryptosystem can make data transmission become more confidential and convenient, both the sender and the recipient must hold the key sets of each other at the same time in order to perform encryption and decryption tasks. Seemingly, it is not practical enough. Therefore, a public-key infrastructure (PKI) method is proposed to solve the practical problem.

A PKI scheme is constructed on the basis of the public-key cryptosystem framework so as to offer all the security requirements, including authentication, confidentiality, message integrity, and non-repudiation. Certificate authority (CA) is a part of the PKI scheme. CA is a trusted third party in the scheme that manages and issues the certificates to the requesters and provides services such as keeping public keys, offering directory service, and issuing certif-

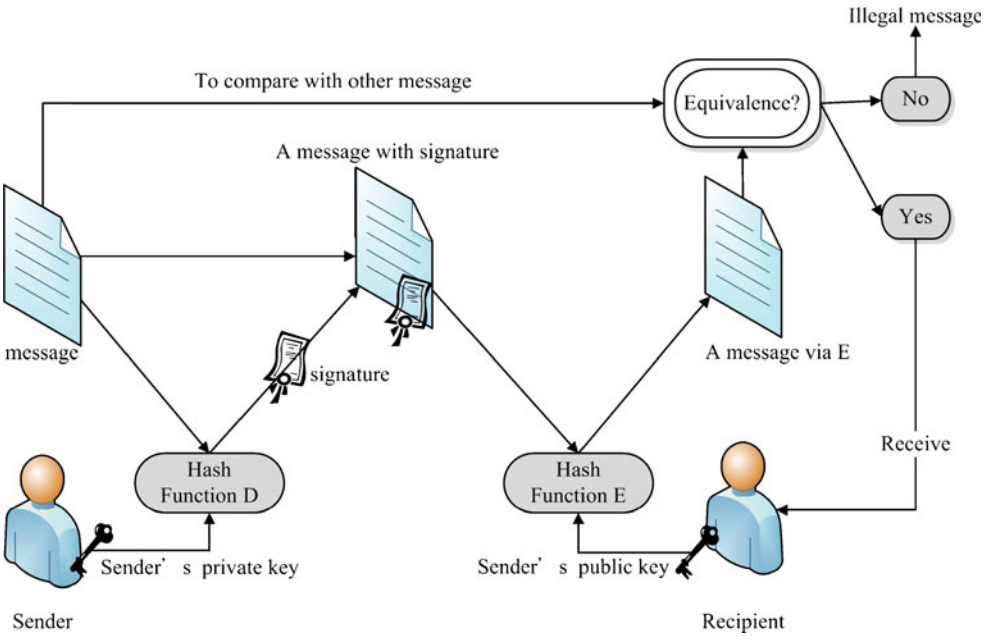

Fig. 1 How a digital signature works under a Public Key cryptosystem

icates. Under the PKI scheme, both of the parties are capable of exchanging information securely and safely with each other on the network.

Concerns on the EMR system

There are two major concerns associated with the establishment of Electronic Medical Record (EMR). They are data confidentiality and data integrity. To measure the success of an EMR system, we have to take those related laws, confidential security and personal privacy issues into considerations. Therefore, we believe it is more important to get these concerns pre-solved before building up a health information system since all the electronic anamnesis must meet the following security requirements: privacy, authentication, integrity, and non-repudiation. In the United States, there are already plenty of cases and discussions under the Health Insurance Portability and Accountability Act (HIPAA). Similar to what has been accomplished in the United States, a number of legislative acts are passed or on the lawmaking process in Europe, like SEISMED [11], NEW-ISO/IEC1018 [12], NVN-NEW12924 [13], NVN-ENV13602 [14].

Data confidentiality

Confidentiality is the most fundamental security requirement for the electronic anamnesis. Medical records are only accessible by authorized parties. Therefore, an identity check must be in place to verify the validity of the requesters to see whether they are authorized to view the patient's confidential information and further to modify the patient's records. Besides, a question to be mentioned here is that how long the requester can access a patient's record and what kind of record he can modify. There is a possibility of having illegal accesses when the requester's certificate is expired. In such situation, it could lead to an abuse and harm the overall security of the system. Thus, to protect the confidentiality of the EMR system, we set up a time stamp on each record so as to trace the time it has been modified and who did it.

Data integrity

Electronic medical records are usually managed under a database system. A good database system can manage all its stored data in terms of the accuracy and unity. For a medical care provider, the system can assist him to create a patient's record, to edit the record after the patient examined, and to retrieve patient's information before he goes to examine. Apart from that, the accuracy and unity of the system can be achieved because any modification or deletion would not be allowed without an authorized permit. In fact, the result of the diagnosis would be added as an appendix on the end of the medical records; thus, the original would not be altered by anyone. An action log will be generated if there is any task performed on the record. Therefore, an action log will document all the things, such as the purpose of a diagnosis, a treatment procedure, patient's examination time, and which location the examination made [15]. Necessarily, the digital signature should be integrated to the electronic anamnesis, because it can help to ensure data integrity and to verify the non-repudiation of the content.

Though an EMR system is implemented, all the protected health information (PHI) through the network should be supervised. The senders and the recipients exchanging information through the network relied upon the digital signature mechanism between both parties to verify. Furthermore, a non-repudiation protocol on the system can prevent the sender from denying the contents that are sent.

Long-term information storability

Health care requires a long-term commitment to preserve the medical records for a number of years as specified by the law. In all probability, a well-constructed EMR system must be able to provide accesses to the records in terms of promptness and accuracy.

The digital signature mechanism can prevent the contents of the electronic documents from any intentional modification during the transmission. However, it is not designed to preserve those documents in a long period of time. Actually, the digital signatures that we are using today can only provide with a short-term guarantee. The certificate issued by the CA is quite similar because the certificate would become invalid due to the revocation or its time expiration. One more question is that when a certificate goes expired, the legitimacy of the digital signature during its validity period doesn't affect. It has much difficulty in proving the time that the digital signature is generated. Is the digital signature generated within the certificate's valid period or out of its validity?

The PKI platform can provide with a time stamp service and support the digital signature mechanism. Time stamp is a technique to act as an independent third party. Its purpose is to provide an exact-time certificate for any electronic document or any electronic transaction so as to ensure that the contents in the document or in the transaction have not been altered after the document or the transaction is stamped. Time stamp service can prove the original document that is created on a specific time point and also a time stamp is an indicator to confirm the

document is secure while its authentication certificate is still within its valid period for the access. After the exact-time certificate has been revoked, the signature would become null and void. However, the holders of the private and public keys are responsible for the signatures to create before the certificate is revoked, according to the rule of non-repudiation. Hence, the keys and all the medical information must be well preserved by the system to allow all the modifications able to be traced later on. The following illustration, Fig. 2, at below gives the procedure of how an electronic document being signed by a time stamp.

Legal concerns on the EMR system

In the past, the patients' records could not be exchanged among medical care providers. Most of the patients probably went into a medical center once and then didn't visit again for their whole life. Thus, the patient's duplicated copies of anamneses should be scattered at the different medical facilities. Because the patient's records are stored here and there, how the doctors can diagnose correctly. At worst, the doctor may misdiagnosis and let the disease get out of control. That's why it is necessary to develop an EMR system to reduce the risk of misdiagnosis. In the future, the patients would have their medical records shared on the network by all medical care providers. When that day comes, no matter which clinic or hospital you go your doctor can examine properly as all sufficient information are on hand. That's the goal we should seek to accomplish. Thus, provided with an appropriate security scheme for the electronic anamneses, the EMR system will become more widely used by the medical facilities. So, everyone can be treated or diagnosed more properly when they are ill.

For example, X-ray examination is one of the most common medical treatments. X-ray image can help the doctors to identify the diseases that can't be seen by the eyes and is also supportive to the doctors on tracing the applied medical treatments. Based upon our research, all the European governments have the laws to require the medical facilities to preserve the patient's X-ray images for at least 30 years. The X-ray image preservation is not easy, because these images may be deteriorated over time due to the cases of high humidity, fire, flood, and insects. So, making the medical documents more storable for a long period of time is essential.

According to the electronic signature law in the Europe, the electronic certificate providers shall preserve all the relating certificates for at least five years. Though the law doesn't require the electronic signature and certificates to be preserved forever, the security of the electronic document would face a breach once the electronic signature is revoked.

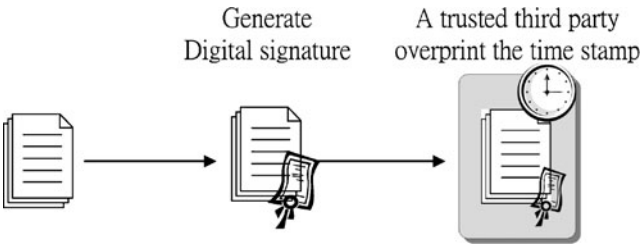

Fig. 2 The procedure of how an electronic document being signed by a time stamp

Proposed solution

The attack from the illegal third parties continues day after day, and never stops. It is crucial to enhance the information security when the data are being transmitted on the open network. Once the information is stolen or tampered by a malicious third party, the consequences could be appalling. For that reason, our scheme can help to solve the problems that are caused by short-lived digital signatures, and certificates. The proposed scheme is to set up a re-signing procedure on a digital signature and all its related certificates, because we believe that letting a digital signature be re-signable can maintain the confidentiality of an EMR system and to extend the storability of all the patients' documents.

The re-signing process

Please note that the re-signing mechanism been proposed by a few scholars before is a procedure to make the digital signature become re-signable before it goes expired. Basically, those previously proposed schemes to solve the overdue issue of a digital signature made the encrypted text

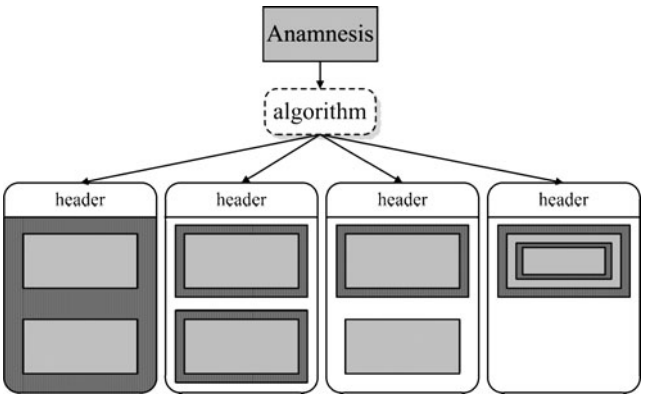

Fig. 3 Proposed electronic anamnesis structure

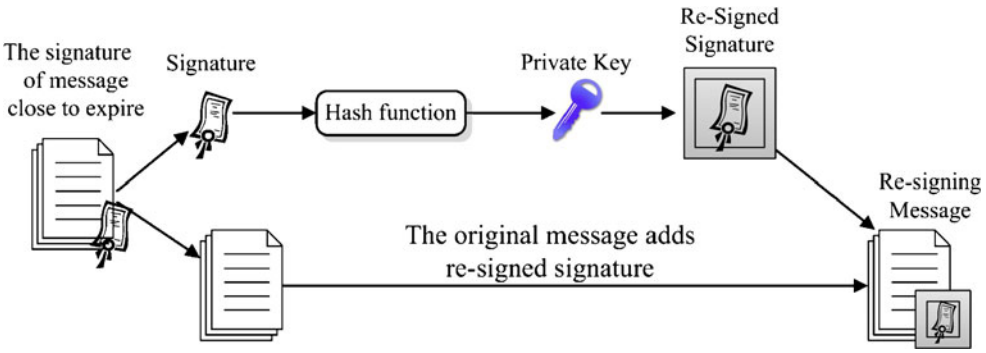

Fig. 4 Re-signing process on an electronic anamnesis

message be decrypted first and then encrypted it again [16–18]. However, this mechanism is not faultless, because it faces two security concerns as below:

1. The decrypted message might have the confidential data revealed to a third party, and which may violate the law.
2. The decrypted message might contain an individual's confidential information, and which could violate the ethics.

Therefore, an improved re-signing mechanism is proposed to solve these problems. The original message will be equipped with a new encryption key and a new signature while the old encryption key and signature are still kept on the file. Thus, the original message can be decrypted by its original key in the future. The electronic anamneses under this mechanism would not violate the law and the ethics. Moreover, the security and integrity of the messages are both protected at the same time.

Re-signing mechanism and MIME

According to the documents published by Joint Commission on Accreditation of Healthcare Organization (JCAH), some may still feel anxious about the use of electronic anamneses, because of the possibility of leakage on patients' information. Regarding to the privacy concern on the electronic medical records, we make the re-signing mechanism combined with the technique of Multipurpose Internet Mail Extensions (MIME) to minimize the worry. MIME is a standard format of E-mail on the Internet. The illustration, Fig. 3, at below is a description of how an electronic document is wrapped by a mathematical algorithm [19].

Figure 3 shows that there are four types of how an anamnesis being wrapped by a mathematical algorithm. In the first type, all the data in an anamnesis is wrapped together. In the second, the data in an anamnesis is wrapped separately. Third, only the particular data selected from the anamnesis is wrapped. The fourth type is much more extraordinary than the others, because some data in an anamnesis is updated and then wrapped at the same time; that is, the essential is bi-wrapped.

The purpose of wrapping is to solve the invalidity issue of the digital signatures. The advantages of using this method are listed as follows:

1. The confidential contents could remain encrypted constantly.
2. Confidential data would be kept safe from the threat of security leakage when re-signing is performed.
3. The original signatures will be not changed; therefore, message can be decrypted by its original signatures.

Wrapping the electronic anamnesis is not only to ensure patients' personal privacy, but also to maintain the integrality of the medical records. After the electronic anamneses have already wrapped securely, only the person by given an authority from medical care providers can log in and perform re-signing. Note that re-signing has no restrictions on the number. Each individual diagnosis of a patient should be well stored and protected for a long period. It is believed that the maintenance of all the original electronic anamneses is more integral and more confidential, and then the patients can get more perfect cares in the future. Regarding to the security of the electronic anamneses, we can use difference algorithms to ensure confidential data will not be stolen by illegal third parties.

Figure 4 at below is to illustrate the process of how the re-signing performed on the digital signature.

Fig. 5 Structure of re-signing mechanisms

First, we declare that the re-signed signature is more secure than the previous one. If the security of re-signed signature is weaker than the previous, then it got the risk that the confidential data would be stolen by the malicious third parties. Second, the re-signing process must be applied repeatedly before the signature is close to expire or to be invalid. If the signature is no longer valid, the re-signing mechanism would be terminated. Finally, we would like to mention a few things that can be done to improve the security level of the signature as we apply the re-signing process (Fig. 5).

1. Use Elliptic Curve Cryptosystem, instead of RSA. Although RSA is the most widely used public-key cryptosystem, it requires a large amount of calculations. Therefore, we suggest Elliptic Curve Cryptosystem, which shows much more advantages than RSA, such as smaller key length, lower computation, and higher processing speed.
2. Use encryption keys in different lengths. If the length is more various, the encrypted strength increases more relatively. Hence, the encrypted information will be too difficult to attack.
3. Use different hash functions or apply new mathematical algorithms. It is more rigorous in the encryption scheme.

Most of the current medical systems encrypted patients' documents in the beginning. If we want to encrypt them again, we must decrypt them first. However, the previous encryption key can't retain and there will be a disclosure risk of patients' documents. Therefore, the paper is to propose a re-signing scheme to avoid the problems mentioned above and protect the integrity and confidentiality of patients' documents. It also corresponds to the rules of HIPAA.

Re-signing is a mechanism to allow the digital signature attached with a re-signable time stamp. With the time stamp technique, we don't worry about the digital signatures going expired. However, to guarantee the signature can be verified after a long period, all related certificates with the original signature must be stored properly. This paper is mainly to focus on the security problem of electronic anamneses in their long-term storability. Therefore, the paper proposed a strategy that makes use of the mathematical algorithms and wrapping methods to perform re-signing, so as to improve the old re-signing mechanism. Finally, the integrity and confidentiality of the electronic anamneses can be kept over a long time.

Conclusions

Electronic anamneses make the health information more convenient to be accessed and transferred between different medical institutions. They are also of higher storability. The EMR itself is embedded with public key infrastructure (PKI) cryptography and digital signature to ensure the security of patients' documents. The database would no longer be accessible after the digital signature becomes expired. Thus, the proposed re-signing mechanism is suitable to be applied to an existing EMR system so as to improve its security in term of data protection. Even though the re-signing mechanism is a workable plan, how to define the signer or the re-signer would be the next issue we shall start thinking about.

Acknowledgement This work was supported partially by National Science Council of Republic of China under Grants NSC 97-2221-E-029-015.

References

1. Institute of Medicine, The computer-based patient record, An essential technology for health care, NAP, Washington, DC, 1991 (revised 1997).
2. Rash, M. C., Privacy Concerns Hinder Electronic Medical Records, The Business Journal of the Greater Triad Area, April 4, 2005.
3. The state of HIPAA privacy and security compliance, AHIMA, April 2005.
4. http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm. Business to modernize.
5. Hospital Administration Commission, Department of Health, 2003.
6. Wang, D. W., Liu, D. R., and Chen, Y. C., A mechanism to verify the integrity of computer-based patient records. *J China Assoc Med Inform*. 10:71–84, 1999.
7. Stallings, W., Cryptography and network security, principles and practice, 3rd edition. Prentice Hall, New York, 2003.
8. ElGamal, T., A public key cryptosystem and signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theories*. 31 (4):469–472, 1985.
9. Peyravian, M., Tusdik, G., and Herreweghen, E. V., A Certification Infrastructure for ATM. *ATM forum/95–0964*, Toronto, 1995.
10. ISO TS 17090 Health Informatics, Public key infrastructure, Part 1, framework and overview, Part 2, certification profiles, Part 3, policy management of certification authority (revised towards an ISO standards by ISO TC 215 WG 4 in 2004).
11. AIM (Advance Informatics in Medicine), Secure Environment for Information Systems in MEDicine, SEISMED (A2033)/SP14/ HILD/05.07. 95.
12. NEN-ISO/IEC 10181, 1996 Information technology, Open System Interfacing (OSI), Security Structures for Open System, Part 1–7.
13. NVN-ENV 12924, 1997 Medical informatics, Division of Security and Protection of Information Systems in Health Care.
14. NVN-ENV 13608, 2000 Medical Informatics, Security of Communication in Health Care, Part 1–3.
15. Blobel, B., and Nordberg, R., Privilege management and access control in shared care health information systems and HER. In: Proceedings of the MIE 2003, Studies in Health Technology and Informatics, Vol. 95. IOS: Amsterdam, 2003.

16. JaJa, J., Robust technologies for automated ingestion and long-term preservation of digital information. *Proc 2006 Int Conf Digital Gov Res, ACM Int Conf Proc Ser.* 151(14):285–286, 2006.
17. Zhang, Z. X., Fang, B. X., Hu, M. Z., and Zhang, H. L., Security analysis of session initiation protocol. *Int J Innov Comput Inform Control*. 3(2):457–469, 2007.
18. Ding, Q., Pang, J., Fang, J. I., and Peng, X. U., Designing of chaotic system output sequence circuit based on FPGA and its applications in network encryption card. *Int J Innov Comput Inform Control*. 3(2):449–456, 2007.
19. Pharow, P., and Blobel, B., Electronic signatures for long-lasting storage purposes in electronic archives. *Int J Medic Inform*. 74 (2):279–287, 2005.