Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Technology 6 (2012) 954 – 961

Procedia Technology

2nd International Conference on Communication, Computing & Security [ICCCS-2012]

Design of RSA-CA Based E-Health System for Supporting HIPAA Privacy-Security Regulations

Sangram Ray[a,*], G. P. Biswas[b]

[a,b]*Department of Computer Science and Engineering, Indian School of Mines, Dhanbad-826004, India*

Abstract

The privacy and the security regulations are two essential requirements of Health Insurance Portability and Accountability Act (HIPAA), recognized by US congress in 1996 as the US Federal Law followed by global e-health industry, in the protection of healthcare privacy. In this paper, a certificate authority (CA) based duality solution has been proposed to fulfill the HIPAA privacy and security regulations that supports both contract and smart card based systems. It presents a patient-centric e-health system based on RSA based public key certificate that allows secure sharing of healthcare information through internet. Doctors and relevant medical staff must have to take patients' permission for online access to patients' PHI data stored in the national medical center server (MCS). A copy of PHI text-data is stored in patients' e-health smart card to support the duality. A random session key is generated in each appointment after prior authentication to upload and retrieve patients' PHI data to or from MCS. One advantage is that the proposed CA based e-health system is easy implementable using existing security standards, tools and products. Discussions regarding the fulfillment of HIPAA regulations and comparison with the existing schemes have been provided to show the better performance of our scheme.

Keywords: Health Insurance Portability and Accountability Act (HIPAA); Certificate Authority (CA); Protected Health Information (PHI); e-health security; Medical Center Server (MCS); Public Key Infrastructure (PKI).

1. Introduction

The implementation of e-health systems and services in all countries with privacy and security is a challenging job which is shared by several health agencies and health authorities at the international, national and local levels. The Health Insurance Portability and Accountability Act (HIPAA) [HIPAA, 1996] are

* Corresponding author. Tel.: +91-8797369171; fax: +0-000-000-0000 .
E-mail address: sangram.ism@gmail.com

doi:10.1016/j.protcy.2012.10.116

recognized by the United States Congress in 1996 as the US Federal Law that applies to the U.S. healthcare industry and may also be applied to other countries with their relevant domestic laws. HIPAA standard [HIPAA, 1996] has not defined how the privacy and security regulations can be accomplished. According to HIPAA's special indication, the patients' privacy should be emphasized and this principle can be applied to the entire health industry throughout the world [Yanga et al., 2006; Collmann et al., 2004].

The privacy and security regulations of HIPAA [HIPAA, 1996] are strongly related and complemented each other to set up guidelines for the protection of patient's privacy and security of health information, a brief discussion of them are given below [Lee and Lee, 2008; Hu et al., 2010]. The *privacy and security regulations* are defined as follows.

- *Patients' understanding*: Patients' right to understand how their PHI data will be used and kept, which contains patient's name, address, contact number and medical record based health information.
- *Confidentiality*: Various software safeguards such as encryption, authentication etc. are described by security regulations to protect health-data during storage and transmissions.
- *Patients' control*: Patients can control the access to their PHI by managing cryptographic keys.
- *Data integrity*: Patients' PHI data should be protected from medical omissions, tampering and unauthorized destruction.
- *Consent exception*: In life-saving purposes and other exceptional situations, the access of the PHI without the patient's authorization is allowed.

To accomplish the above requirements, three cryptographic mechanisms have been proposed so far and they are explained below in brief [Lee and Lee, 2008; Hu et al., 2010; Huang and Liu, 2011].

In 2008, Lee and Lee [Lee and Lee, 2008] proposed a smart card based cryptographic key management scheme for HIPAA privacy and security regulations. Several limitations of this scheme have been found and observed as the scheme is session based and requires the presence of the smart card for each access to the PHI which is unrealistic, and patients cannot freely change their own passwords of smartcards. The major problems of this scheme, like other smart card based systems, are that it cannot authenticate the presenter of the smart card and the multiple accesses to the PHI by different people from different locations are not supported during the whole medical treatment process. This scheme also not supports the recent paper based e-health system environment, where the patients' PHI data is entirely left to the medical service provider such as a hospital that grants the every access to it after secure authorization, and each patient signs a fixed time-period contract with the hospital to allow the access of his PHI data.

To establish the contract-oriented system, J. Hu et al. [Hu et al., 2010] proposed a hybrid public key infrastructure solution (HPKI) for HIPAA privacy and security regulations in 2010. In this scheme, a smartcard trust centre (STC) issues medicare smart cards to each patient and patients' PHI data is entirely left to the medical centre server (MCS) during the contract period. Some limitations of this scheme have been observed such as this scheme is out of patients' control since relevant medical service providers have unlimited access to the PHI in patients' absence. Also no clear procedure is given for consent exception cases and treatment in foreign countries.

In 2011, Huang and Liu [Huang and Liu, 2011] proposed a new smart card based key management scheme for HIPAA privacy and security regulations in elliptic curve cryptosystem (ECC). In this scheme, instead of RSA, ECC has been used to minimize the key size and computation cost for registration, signature verification and encryption-decryption processes. It generally follows Lee and Lee's scheme so that all the limitations of the same exist except allowing patients to freely choose and update their passwords.

This paper presents a new patient-centric e-health architecture for supporting both the contract oriented and smart card based systems. In brief, a national medical centre server (MCS) is considered to store all relevant data including a patient's PHI data, which is not accessible without the patient's permission. After authentication with the MCS, each patient, doctors and relevant medical staff register for treatment, access and/or upload patients' PHI data etc to the MCS using a temporary secret session key and after completion of treatment, the complete PHI data is uploaded to MCS, where a copy of the PHI text-data is stored in patients' e-health smart card. For authentication of different entities, the proposed scheme uses the RSA based public-key

certificate issued by certificate authority (CA) [Weise, 2001; NIST, 2001; Elgamal, 1985; Stalings, 2009] and a symmetric encryption-decryption for PHI data transmission. The proposed technique can also support the patients' emergency condition and the treatment in foreign countries. One of the advantages is that the proposed e-health system is implementable using existing cryptographic security standards, tools and products. A discussion also added here regarding the fulfilment of the HIPAA security/ regulations followed by a comparison with the existing schemes proposed so far.

The remaining parts of this paper are organized as follows. In section 2, the CA based e-health system is proposed to fulfil the HIPAA privacy and security regulations. Discussions regarding how the proposed scheme fulfils the HIPAA regulations and a comparative study with existing schemes are given in section 3. Finally, section 4 concludes the importance of the proposed scheme.

2. Proposed RSA-CA based e-health system

In our proposed e-health system, each patient, doctor and relevant medical staff have their own public key certificate. Each patient has to register at the national medical center server (MCS) to get e-health service provided by the national medical service provider. The MCS has its own database and stores all relevant data including patients' PHI data which is not accessible without patient's permission. Patients and medical staffs get access to the MCS through internet with prior patients' permission except emergency situation. Foreign medical service providers can access the patients' PHI data either through internet to cover telemedicine cases or through patients' smart card to provide treatment at foreign countries. The details of the proposed scheme are addressed below, where the following notations are used:

$h(\_)$: A one-way hash function (e.g. SHA1); (PR_P, PU_P) : Private/public key pair of patient;
(PR_{DOC}, PU_{DOC}) : Private/public key pair of doctor; (PR_{MCS}, PU_{MCS}) : Private/public key pair of MCS;
CA_{MCS} : Public key certificate of MCS; ID_P : Identity of patient; ID_{DOC} : Identity of Doctor;
CA_P : Public key certificate of patient; R_{DOC} : Nonce of doctor; R_P : Nonce of patient;
CA_{DOC} : Public key certificate of doctor; K_S: Secret session key; R_{MCS} : Nonce of MCS;
K_{REG} : Registration key of patient; E : Encryption; D : Decryption;

2.1. The proposed scheme

The proposed scheme is divided into five phases, namely registration, PHI data generation and upload, PHI data retrieval in general and emergency situation and foreign treatment, which are now addressed below.

2.2.1 Registration Phase

A patient has to provide his certificate and his identity to register with the MCS. After receiving these, MCS completes the mutual authentication and creates patient's contract *w,* which is public and consists of the signed consent, the data received from the patient etc. The MCS then computes patient's registration key $K_{REG} = h(w||k)$ where, $k \in Z_q$ is a random number, as shown in Fig 1.

Step 1: *Patient → MCS:* ID_P, *reg. req,* CA_P, R_P

A patient sends his *registration request* with his public key certificate, identity and a nonce R_P to the MCS. On receiving, MCS validates patient's certificate and retrieves the public key with timestamp.

Step 2: *MCS → Patient:* $E_{PU_P}(R_{MCS}, R_P)$, CA_{MCS}

In response, MCS encrypts his challenge R_{MCS} to authenticate the patient together with R_P using the patient's public key, and sends the same and its own public key certificate to the patient.

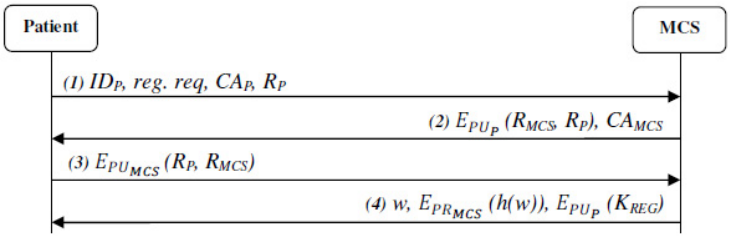

Fig. 1. registration phase

Step 3: *Patient → MCS:* $E_{PU_{MCS}}$ (R_P, R_{MCS})

After receiving, patient validates the MCS's certificate, retrieves its public key, decrypts the encrypted message using his private key and gets back his own challenge and MCS's challenge R_{MCS}.

Now the patient sends a reply message by encrypting using MCS's public key to complete the mutual authentication, where the order of R_P and R_{MCS} is switched to prevent the replay attack.

Step 4: *MCS → Patient: w,* $E_{PR_{MCS}}$ *(h(w)),* E_{PU_P} *(*K_{REG}*)*

MCS receives the reply message, decrypts it using its private key and gets back its own nonce sent that confirms the patient's authenticity. The MCS then creates the patient's contract w consisting of the signed consent, the data received from the patient etc, and generates the registration key $K_{REG} = h(w||k)$ where, $k \in Z_q$ is a random number. Since w is public, MCS sends it directly to the patient together with the signed hash value of w for integrity and as a proof of the legality of the contract. The patient's registration key is stored at MCS and a copy is sent to the patient encrypted with patient's public key to ensure that only patient will get it.

2.2.2 PHI data generation and upload procedure

The PHI data generation and upload procedure is sequentially divided into two phases, namely temporary secret session key generation and PHI data generation and upload.

2.2.2.1 Temporary secret session key generation

For each appointment of a patient with any doctor trusted by the MCS, doctor/MCS generates a random secret session key K_S and negotiates it for that particular period. The K_S is temporary and is deleted at the end of each appointment. For a new appointment with any doctor, a new temporary K_S is generated.

2.2.2.2 PHI data generation and upload

When a patient meets any doctor for treatment purposes, the doctor generates a temporary secret session key K_S, treats the patient and generates the patient's PHI data. The PHI data are categorized namely text-data and image-data. The PHI text-data consists of sensitive textual data of less size including the patient's name, address, medical test results etc, and image-data consists of large volume of medical images. After generating the patient's PHI data, the doctor sends the patient's PHI data *upload request* to the MCS and uploads the signed and encrypted data as shown in Fig 2 and illustrated as follows:

Step 1: *Doctor → MCS:* ID_{DOC}, *upload req,* ID_P, CA_{DOC}, R_{DOC}

A doctor sends the patient's PHI data *upload request* with his identity, certificate, the patient's identity and a nonce R_{DOC} to MCS. After receiving, MCS validates the doctor's certificate and retrieves the doctor's public key.

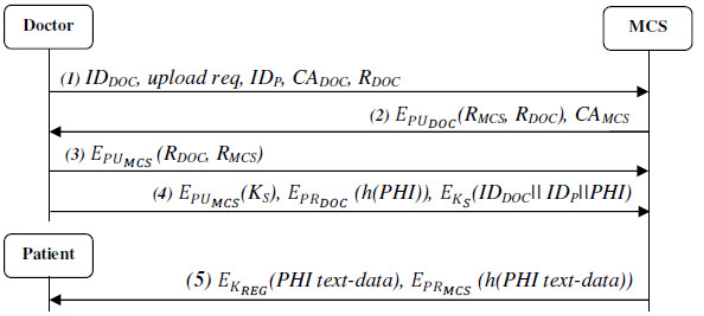

Fig. 2. PHI data uploading protocol

Step 2: *MCS → Doctor:* $E_{PU_{DOC}}$ $(R_{MCS}, R_{DOC}), CA_{MCS}$

In response, MCS generates a challenge R_{MCS}, encrypts it with R_{DOC} using doctor's public key and sends it with its certificate to the doctor.

Step 3: *Doctor → MCS:* $E_{PU_{MCS}}$ (R_{DOC}, R_{MCS})

After receiving, the doctor validates the MCS's certificate, retrieves its public key, decrypts the encrypted message using his private key and gets back his own challenge, which confirms that MCS is authenticated. Now to be authenticated to MCS, the doctor sends a reply message encrypted using MCS's public key and the order of R_{DOC} and R_{MCS} is switched to prevent a replay attack.

Step 4: *Doctor → MCS:* $E_{PU_{MCS}}$ (K_S), $E_{PR_{DOC}}$ $(h(PHI))$, E_{K_S} $(ID_{DOC}||ID_P||PHI)$

MCS gets the reply message, decrypts using its private key and gets back the same nonce which confirms the mutual authentication. Now the doctor generates a temporary secret session key K_S and sends it to MCS encrypted using MCS's public key for negotiation. The doctor also concatenates the patient's PHI data with doctor's identity and patient's identity, encrypts the concatenated message using K_S and sends the same and signed hash digest of PHI to the MCS as message 4.

Step 5: *MCS → Patient:* $E_{K_{REG}}$ $(PHI\ text\text{-}data)$, $E_{PR_{MCS}}$ $(h(PHI\ text\text{-}data))$

After receiving, MCS uses the session key K_S obtained by decrypting with his private key, to decrypt the encrypted message, gets the patient's PHI, and identity of the patient and the doctor. Now MCS compares the identities of patient and doctor, if both are same, then the MCS calculates the hash digest of the PHI data and compares it with the signed hashed PHI data sent by the doctor. If it passes, MCS stores the patient's PHI with the patient's identity and deletes the temporary key K_S.

After uploading, MCS sends a copy of PHI text-data to the corresponding patient. For this, MCS encrypts the uploaded PHI text-data using patient's registration key, puts a signature on PHI text-data, and sends the encrypted message with the signed value to the patient. Now the patient decrypts the message using K_{REG}, gets the PHI text-data, calculates the hash digest, and compares it with the received signed hashed PHI text-data. If passes, the patient stores the PHI text-data in his smart card.

2.2.3 PHI data retrieval procedure

During any treatment period, the doctor may require the previous PHI data stored at MCS. To do this, the doctor sends a PHI data *retrieve request* to MCS and follows the internal authentication procedure. After receiving the PHI data *retrieve request*, the MCS generates a new temporary secret session key K_S with the doctor and sends the encrypted patient's PHI data to the doctor. The procedure to retrieve the patient's PHI data from MCS through PHI data retrieval protocol is shown in Fig 3 and illustrated as follows:

Step 1 to *step 3* are same as the PHI data uploading protocol discussed in *Sec. 2.2.2.2* except that instead of

uploading request, the doctor sends the PHI data *retrieve request* to MCS at step 1.

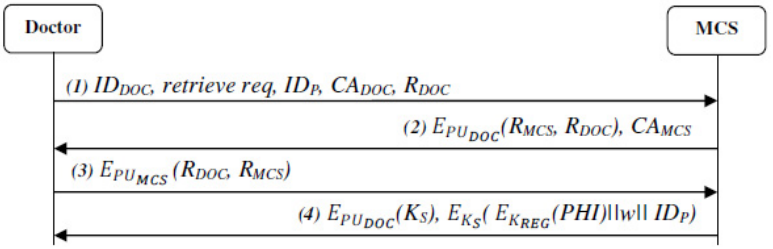

Fig. 3. PHI data retrieval protocol

Step 4: *MCS → Doctor:* $E_{PU_{DOC}}(K_S)$, $E_{K_S}(E_{K_{REG}}(PHI)||w||ID_P)$

MCS receives the message 3, decrypts it using its private key and gets back the same nonce which confirms that the mutual authentication is completed. Now the MCS generates a temporary secret session key K_S and sends it to the doctor encrypted using the doctor's public key. It also encrypts the patient's PHI data using patient's registration key, concatenates it with w and patient's identity, encrypts the concatenated message using K_S, and then sends the same to the doctor as message 4.

After receiving the message 4, the doctor decrypts the encrypted K_S using his private key and gets K_S. Now he decrypts the encrypted message using K_S and gets the encrypted PHI. Since the patient's PHI data is encrypted using patient's registration key, so the doctor cannot access it in patient's absence. This supports our aim i.e. patient's PHI data is not accessible without patient's permission. To make accessible it, the patient decrypts the encrypted PHI data by using his registration key secretly. The patient can also provide his PHI text-data directly to the doctor using his smart card.

During this treatment period, if the doctor wants to upload the patient's new PHI data, he can upload the signed and encrypted PHI data to MCS using the same K_S of that appointment through PHI data uploading protocol as shown in Fig 2. At the end of the appointment, the MCS deletes the K_S as previously discussed.

2.2.4 PHI data retrieval in emergency period

In patients' emergency/consent exception cases, the doctor sends an emergency PHI data retrieve request with the patient's identity to the MCS. The procedure to retrieve the patient's PHI data from the MCS in patient's emergency condition is shown in Fig 4 and illustrated as follows:

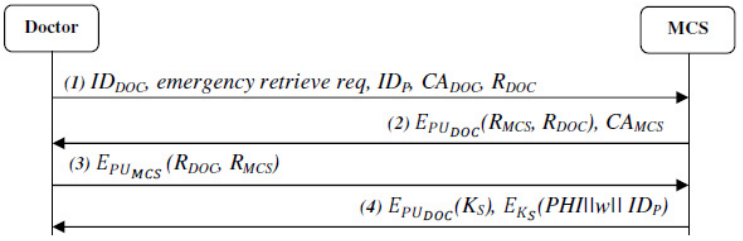

Fig.4. PHI data retrieval in emergency period

After receiving the *emergency PHI data retrieve request* from a doctor, the MCS initially authenticates the doctor followed by *step 1* to *step 3* of PHI data uploading protocol discussed in *Sec. 2.2.2.2*.

Step 4: $E_{PU_{DOC}}(K_S)$, $E_{K_S}(PHI||w||ID_P)$

After completion of mutual authentication, MCS generates a temporary secret session key K_S and sends it to the doctor encrypted using doctor's public key. The MCS also encrypts the patient's PHI

data, the contract w and the patient's identity using K_S, and sends it to the doctor. The doctor decrypts using his private key and gets the K_S and then decrypts the message using K_S to get PHI data.

During the emergency period the doctor cannot upload the patient's new PHI data since patient is not in sense. When patient is in sense, the doctor uploads the signed and encrypted data to MCS through PHI data uploading protocol as shown in Fig 2 using the same K_S of that appointment.

2.2.5 Foreign access of patients' PHI

In foreign countries, a patient has to provide his public-key certificate, his identity and his nationality to the foreign MCS. After receiving these, the foreign MCS completes the mutual authentication procedure and creates a patient's contract w' consists of the signed consent, the data received from the patient etc. Now the foreign MCS computes patient's registration key $K_{REG}' = h(w'||k')$ where, $k' \in Z_q$ is a random number and follows the PHI data upload and retrieval protocol as shown in Fig 2 and Fig 3. During this treatment process the foreign doctor can access the patient's previous PHI data from the patient's smartcard, and at the end of the treatment, a copy of the new PHI data is stored in the patient's smart card.

3. Fulfillment of HIPAA regulations and comparison with other schemes

In this section, the fulfillment of the HIPPA privacy-security regulations in our proposed e-health scheme and its comparison with the existing three schemes are given in following two sub-sections.

3.1 Fulfillment of HIPAA regulations

In order to describe the fulfillment of HIPAA privacy and security regulations, the summarized regulations [Lee and Lee, 2008; Hu et al., 2010; Huang and Liu, 2011] and their corresponding implementations are explained below:

- *Patient's understanding*: In our scheme, a signed permission either in paper or electronically is required from patients to register at the MCS. This sets up the terms and regulations regarding how their PHI data will be accessed and stored in MCS according to the security protocols illustrated above. It also explains how his PHI data can be retrieved in his emergency situation.
- *Confidentiality*: The randomly generation of temporary secret session key K_S ensures that the session key is securely generated by the doctor with the patient's physical presence and negotiated with MCS by encrypting it with MCS's public key. To upload or retrieve, the PHI data is encrypted using K_S to obtain confidentiality. The CA based authentication protocols discussed above provide cryptographic security against unauthorized access of patient's PHI. So it is reasonable to assure that the confidentiality of the patient's PHI is obtained in our scheme.
- *Patient's control*: In our scheme, the permission to upload and retrieve the patient's PHI data is controlled by the MCS and the patient. To decrypt the encrypted PHI, the corresponding temporary secret session key K_S, which is encrypted using the patient's public key, must be obtained. Although K_S is not sufficient to retrieve the PHI data since it is also encrypted using patient's registration key which is unknown to the doctor. So, the patient's consent must be needed. Thus the proposed scheme is under patient's control.
- *Data integrity*: In our proposed scheme, the PHI data is encrypted using K_S and the patient's registration key, so no one can alter it. Also, in each uploading and retrieval phase, a signed hash digest of PHI data is also sent to ensure the data integrity and data redundancy. The patient's consent against respective K_S cryptographically ensures the non-repudiation.
- *Consent exception*: The proposed scheme provides the security control in life-saving emergency cases, where a clear procedure is given to retrieve a patient's PHI data in emergency situation.

Thus our proposed e-health system fulfils the privacy and security regulations of HIPAA.

3.2 Comparison

So far, only three e-health systems have been proposed in the literature [Lee and Lee, 2008; Hu et al., 2010; Huang and Liu, 2011], and their introduction, analysis and shortcomings are already given earlier, and as a remedy, a contract based scheme based on the RSA algorithm and public key certificate is proposed in this paper. Since the MCS is connected and accessible through internet, any medical staff can use MCS online for accessing and/or uploading the patients' PHI data from any different geographical location. However, no one can access the patients' PHI data without the patients' permission and also a patient does not need to carry the PHI for his treatment although a copy of the same is stored in a patient's smart card as a support for the duality of the PHI data. Now, a comparison table is provided, where a feature-based comparison of the proposed scheme with other existing schemes is reported that shows overall better performance than others.

Table 1. Comparison of proposed scheme with existing schemes

Parameters	Lee and Lee, 2008	Hu et al., 2010	Huang and Liu, 2011	**Proposed Scheme**
Avoidance of Replay Attack	No	No	No	**Yes**
Patient's consent to upload and retrieve PHI data	Yes	No	Yes	**Yes**
Patient's consent during foreign treatment	No	No	No	**Yes**
Clear specification to retrieve PHI data in Emergency	No	No	No	**Yes**
Duality (smartcard and/or MCS)	No	No	No	**Yes**

4. Conclusion

A contract oriented and RSA-CA based solution for supporting HIPAA privacy and security regulations for online e-health systems is proposed in this paper, where a duality solution for PHI data is organized. The online access of the patients' PHI data from MCS is controlled in terms of authentication, encryption, non-repudiation etc. The procedures are also given to handle the patients' emergency situation and to support the treatment in foreign countries. A comparative study is made that shows the importance and easy implementation of our proposed scheme using available tools/software.

References

1996a. Health Insurance Portability Accountability Act of 1996 (HIPAA). Centers for Medicare and Medicaid Services, Available: http://www.cms.hhs.gov/hipaageninfo (online).

Health Insurance Portability and Accountability Act of 1996, 104th Congress, Public Law 1996; p.104–91.

Yanga, C.M., Lina, HC., Changb, P., Jianc, WS., 2006. Taiwan's perspective on electronic medical records' security and privacy protection: Lessons learned from HIPAA, Computer Methods and Programs in Biomedicine 82(3), p. 277–82.

Collmann, J., Lambert, D., Brummett, M., DeFord, D., Coleman, J., Cooper, T., 2004. Beyond good practice: Why HIPAA only addresses part of the data security problem, Int. Congr. Ser. 1268: 113–8.

Lee, WB., Lee, CD., 2008. A cryptographic key management solution for HIPAA privacy/security regulations, IEEE Transactions on Information Technology in Biomedicine 12(1), p. 34–41.

Hu, J., Chen, H., Hou, T., 2010. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations, Computer Standards & Interfaces 32, p. 274–80.

Huang, HF., Liu, KC., 2011. Efficien key management for preserving HIPAA regulations, Journal of Systems and Software 84, p. 113-9.

Weise, J., 2001. Public Key Infrastructure Overview, Sun PSSM Global Security Practice, Sun Blue Prints™ Online - August 2001.

Introduction to Public Key Technology and the Federal PKI Infrastructure, National Institute of Standards and Technology, Feb 26, 2001.

ElGamal, T., 1985. A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transaction on Information Theory 31(4), p. 469– 72.

Stallings, W., 2009. Cryptography and Network Security: Principles and Practices, 4th Edition, PHI, 2009 International Edition, p.420-30.