

A HYBRID PUBLIC KEY INFRASTRUCTURE SOLUTION (HPKI) FOR HIPAA PRIVACY/SECURITY REGULATIONS

Jiankun Hu, Hsiao-Hwa Chen[†], and Ting-Wei Hou

[†]Corresponding Author's Address:

Hsiao-Hwa Chen

Department of Engineering Science

National Cheng Kung University

1 Da-Hsueh Road, Tainan City, 70101 Taiwan

Tel: +886-6-2757575 ext 63320

Fax: +886-6-2766549

Email: hshwchen@ieee.org

Jiankun Hu (e-mail: jiankun.hu@rmit.edu.au) is with the School of Computer Science and IT, RMIT University, Melbourne 3001, Australia. Hsiao-Hwa Chen (e-mail: hshwchen@ieee.org) and Ting-Wei Hou (e-mail: [hou@nc.es.ncku.edu.tw](mailto:hhou@nc.es.ncku.edu.tw)) are with the Department of Engineering Science, National Cheng Kung University, Tainan City, 70101 Taiwan.

The paper was submitted on 30 January 2008 and revised on April 27, 2009.

Abstract

The Health Insurance Portability and Accountability Act (HIPAA) has set privacy and security regulations for the US healthcare industry. HIPAA has also established principles for security standards that global *e*-health industry tends to follow. In this paper, a hybrid public key infrastructure solution (HPKI) is proposed to comply with the HIPAA regulations. The main contribution is the new *e*-health security architecture that is contract oriented instead of session oriented which exists in most literatures. The proposed HPKI has delegated the trust and security management to the medical service provider during the contract period, which is more realistic. It is much an analogy to existing paper based health care systems in terms of functional structure. The cryptographically strong PKI scheme is deployed for the mutual authentication and the distribution of sensitive yet computational non-intensive data while efficient symmetric cryptographic technology is used for the storage and transmission of high volume of medical data such as medical images. One advantage is that the proposed HPKI can be constructed from existing cryptographic technologies where various relevant security standards, tools and products are available. Discussion has been provided to illustrate how proposed schemes can address the HIPAA privacy and security regulations.

Index Terms

e-health security, standard, PKI, smartcard.

I. INTRODUCTION

e-health refers to the Internet-enabled healthcare applications involving management of personal health records or information, and other Internet-based services including *e*-Pharmacy etc. Due to the ease of global access to the information systems, privacy and security is becoming a major concern in the *e*-health systems. In 1996 the Health Insurance Portability and Accountability Act (HIPAA) was established as the US Federal Law regulating US healthcare industry. A central part of the HIPAA standard is privacy and security regulations. However, this federal mandate has not defined how these requirements can be achieved. An increasing effort has been made in the area of healthcare information technology adoption and healthcare data interoperability for secure and seamless sharing of healthcare information [1-6][13-15].

Bhatti *et al.* (2007) [4] proposed a policy-based system to address the following requirements: 1) the integration of privacy and disclosure policies with well known healthcare standards used in the industry for the purpose of producing precise requirements of a practical healthcare system, and 2) the provision of ubiquitous healthcare services to patients using the same infrastructure that can enable federated healthcare management for organizations. More specifically, the disclosure and privacy policies have been designed by making use of requirements specification based on a set of use cases for the Clinical Document Architecture (CDA) standard. Also, a context-aware policy specification language has been proposed, which allows encoding CDA-based requirements use cases into privacy and disclosure policy rules. Unfortunately, the HIPAA security regulations are not covered in this framework.

In order to address both HIPAA privacy and security regulations, a summary of requirements specified in HIPAA privacy and security regulations is provided as follows [6-7].

A. Privacy Regulations

Privacy regulations specify requirements regarding the patients' rights to understand and control the use and disclosure of their protected health information (PHI). The PHI includes a patient's name, address, contact number, and information related to the medical record [6-7].

B. Security Regulations

The security regulations can be summarized as follows:

- 1) Patient's Understanding: The HIPAA mandates that patients have the right to understand how their PHI will be used and kept.
- 2) Confidentiality: Security regulations describe various software safeguards such as encryption for health-data confidentiality during storage and transmission.
- 3) Patient's Control: By controlling cryptographic keys, patients can control the access to their PHI.
- 4) Data Integrity: Medical omissions, tampering, and unauthorized destruction of health information are prohibited.
- 5) Consent Exception: The use and disclosure of the PHI without the patient's authorization are allowed for life-saving purposes and in other exceptional situations.

Intuitively, a smartcard based cryptographic system appears to be a promising solution [1][6]. In [1], a patient-centric content protection system was suggested which is based on temper-resistant hardware and popular security protocols for authentication and encryption. High availability and interoperability of the electronic health record (HER) content protection system is achieved by the use of a specially designed device called Personalized Media Recorder (PMR). A symmetric cryptosystem such as AES (Advanced Encryption Standard) is used. However cryptographic analysis of the proposed overall scheme was not adequately provided.

In [6], a comprehensive cryptographic key management scheme based on the smartcard technology was proposed. The proposed architecture consists of a trusted server of the governmental healthcare office (SG), a server of a health provider (SH), and the patient. The patient registers at SG and then creates a contract. For encryption, the health data card will generate a session key by hashing a combination of its master key, identification of the healthcare provider and a de-identification such as the service number that is unique in the entire health information of the patient. For consent decryption, the patient reproduces the session key based on the master key stored in the smart card, identification of the health care provider and its service number. For consent exception case, the master key can be recovered by sending the patient's public data to the SG. This scheme requires the presence of the smart card for each access to the record which is unrealistic. Quite often, multiple accesses to the PHI are needed by different people during the whole medical treatment process. Medical test-sample analysis laboratories can be geographically separated from the outpatient location. In the current paper based medical care practice environment, the patient's PHI is entirely left to the medical service provider such as a

hospital. As the hospital needs the convenience of the access to the PHI during the whole medical treatment process including the period beyond the outpatient process, it is more appropriate to sign a fixed time-period contract with the hospital and make sure every access to the PHI during the medical treatment process is securely authorized by the hospital and also recorded for non-repudiation purpose.

In this paper, a hybrid public key infrastructure (HPKI) scheme is proposed to address above important issues. The main contribution is the new *e*-health security architecture that is contract oriented instead of session oriented which exists in most literatures. The proposed HPKI has delegated the trust and security management to the medical service provider during the contract period, which is more realistic. It is much an analogy to existing paper based health care systems in terms of functional structure. The cryptographically strong PKI scheme is deployed for the mutual authentication and the distribution of sensitive yet computational non-intensive data, while efficient symmetric cryptographic technology is used for the storage and transmission of high volume of medical data such as medical images. One advantage is that the proposed HPKI can be constructed from existing cryptographic technologies where various relevant security standards, tools and products are available. Discussion has been provided to illustrate how the proposed schemes can address the HIPAA privacy and security regulations.

The remaining structure of this paper is outlined as follows. In Section II, a hybrid PKI based scheme is proposed to address the HIPAA privacy and security regulations. Section III is for discussions about the HIPAA compliance. Section IV is devoted to the conclusions and future works.

II. A HYBRID PKI BASED SCHEME FOR ADDRESSING HIPAA PRIVACY AND SECURITY REGULATIONS

A general architecture for the *e*-health system security is shown in Fig. 1. In this system, we have a smartcard trust center (STC) that issues medicare smartcards. A national medical care organization can provide this service. A medical center server (MCS) belongs to the place where a patient registers as the home medical service provider. The MCS has its own database which stores all relevant data including its patients PHI data. Medical staff and patients get access to the system through the organizational terminals that are considered as physically secure. In

order to cover the cases of telemedicine and geographically separated medical organizations, public network (Internet) is used for the connection to the foreign medical service provider. In the remaining of this paper, the following notations are adopted.

- 1) (K_{pr}^x, K_{pu}^x) refers to (private key, public key) pair of party x in the PKI system;
- 2) K_s denotes the shared secret key s in the asymmetric encryption system.

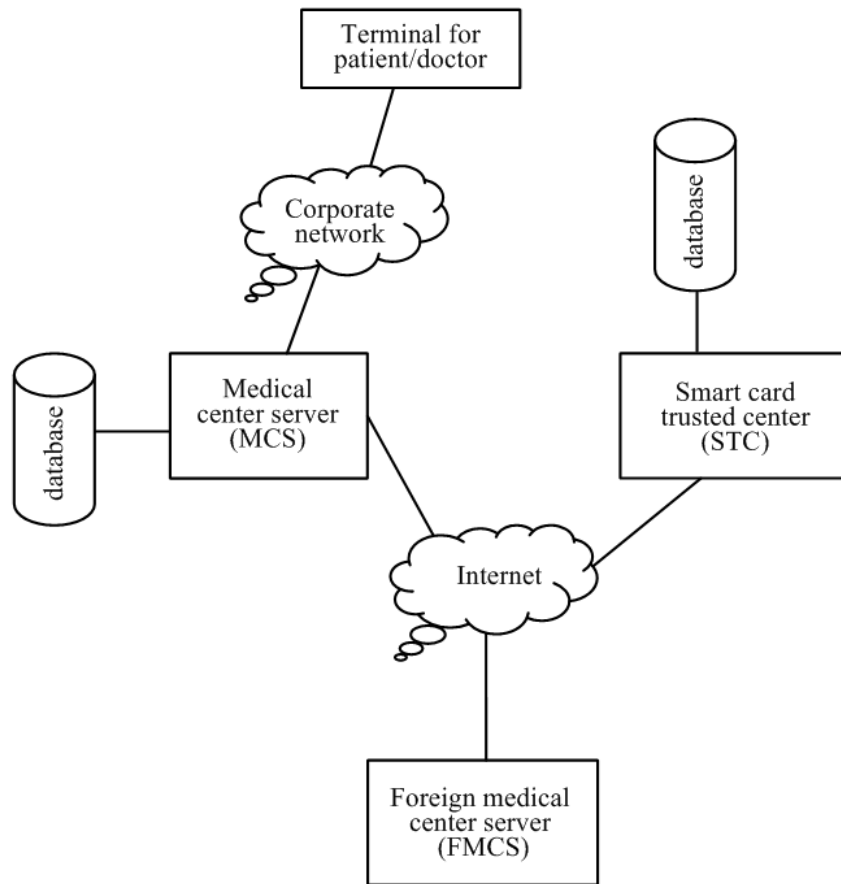


Fig. 1. General architecture of the *e*-health security system.

The proposed hybrid PKI scheme consists of three parts, namely registration, PHI data upload and the PHI data retrieval, which will be explained in the sequel.

A. Registration

1) *Registration with STC*: Similar to the operation of many national medical care systems, a legitimate recipient of the medical care service will need to register with the STC. A smart

medical care card or *e*-health card will be issued and contains the patient's private-public key pair and other basic data. As a trusted center, the STC center will maintain the private-public key pair of the patient. A biometric authentication system can also be embedded for stronger security. A physical presence is needed for the registration which will minimize the security risk at this phase. For instance, patient A will obtain an *e*-health smartcard which contains the patient A's personal information and PKI pair (K_{pu}^A, K_{pr}^A) . Each medical service provider needs to register with the STC center that provides a secret-public key pair $(K_{pu}^{mcs}, K_{pr}^{mcs})$. When people register at the STC, a contract should be signed either in paper or electronic form regarding the terms and conditions how the smart *e*-health card should be used. When it comes to the processing of the medical care service provider's application, a license can only be issued for those who have implemented satisfactory security mechanisms such as what have been proposed in this paper. For management purpose, an audit and accreditation process should be conducted regularly by the third party to monitor the whole *e*-health security system.

2) *Internal registration*: Similar to the registration process with the STC, a medical personnel within a medical care service provider such as a hospital needs to register with the organization and will be issued an organizational smart *e*-health card containing his/her (public, private) key pair.

B. PHI Data Generation and Upload within a Medical Care Center

1) *Contract key generation*: When receiving medical service in the medical center for the first time, a patient has to register with the medical center. For example, the patient A and the MCS will sign a temporary contract which will set the terms of the PHI data use and protection. Specifically, the contract allows the medical center unlimited access during this medical service period to the PHI data under the condition that the MCS implements necessary security mechanisms. These security mechanisms are audited and accredited by the STC. The contract also provides explanations regarding the operation of these privacy and security mechanisms. The signing of this contract will generate a contract cryptographic key as shown in Fig. 2. The contract also sets an expiry date after which the access from the MCS to the PHI data should be blocked unless a new contract is signed or in exceptional cases. Normally, this contract period refers to the time framework that is needed for the treatment of a particular illness which is estimated by the medical center.

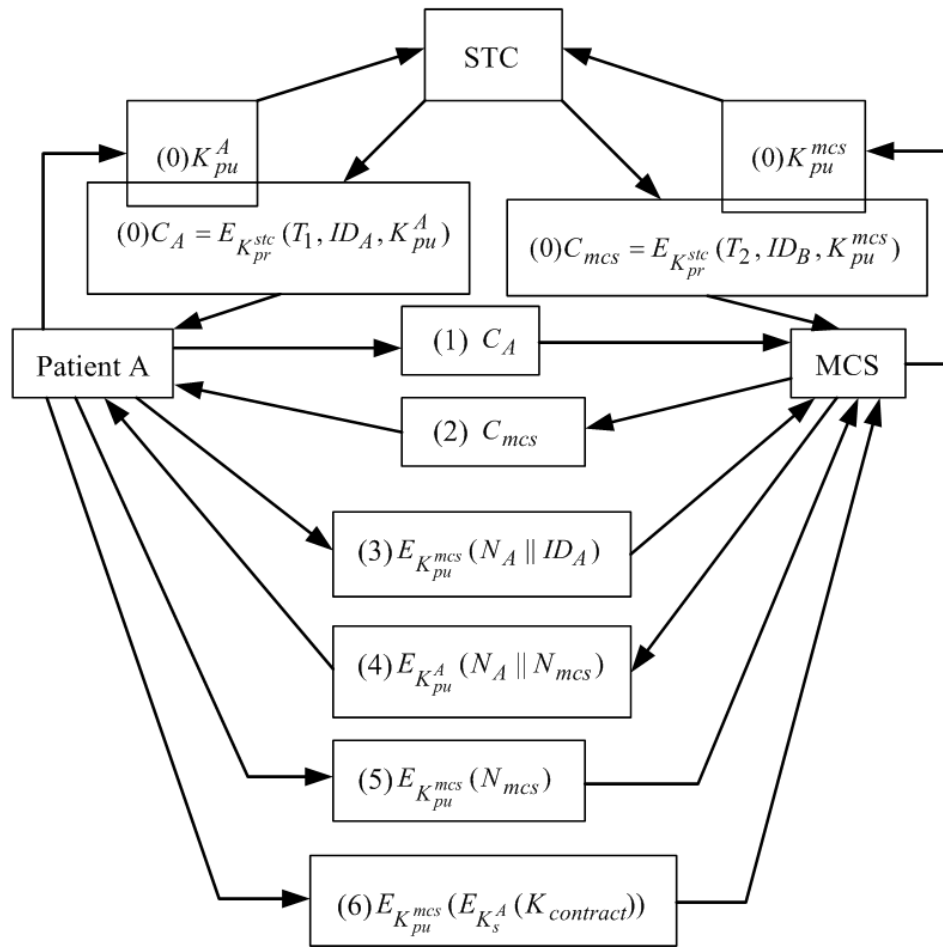


Fig. 2. Contract key generation.

Based on the PKI theory [9][12], a cryptographic contract key is generated as shown in Fig. 2, which is illustrated as follows:

- Step 0: Patient A provides his public key K_{pu}^A to the STC. As Patient A has already registered with the STC, the STC can send a certificate to A via the message $C_A = E_{K_{pr}^{stc}}(T_1, ID_A, K_{pu}^A)$. A has the STC's public key K_{pu}^{stc} via secure channel, e.g., in physical presence in the registration process. Similarly, the medical service provider MCS will get its own certificate $C_{mcs} = E_{K_{pr}^{stc}}(T_2, ID_B, K_{pu}^{mcs})$ and the STC's public key.
- Steps 1 and 2: A and MCS will exchange the certificates. For the MCS, it can decrypt both certificates as it possesses the STC's public key K_{pu}^{stc} via secure channel, e.g., during physical presence of the registration process. It is then assured that K_{pu}^A retrieved from the

certificate $C_A = E_{K_{pr}^{stc}}(T_1, ID_A, K_{pu}^A)$ is indeed the public key from the patient A. This is because that only STC can create A's certificate with STC's private key according to the PKI characteristics. The same applies to the STC's certificate received by A. The timestamp controls the validity period of the certificate.

- Step 3: Patient A will send the message $E_{K_{pu}^{mcs}}(N_A \parallel ID_A)$ to the MCS. This message contains the patient's ID_A and a nonce N_A which are encrypted using the MCS's public key. Only MCS can decrypt this message.
- Step 4: Upon receiving message 3, the MCS is notified that the patient A wants to establish a contract key. But it has not authenticated the patient A yet. Therefore, it sends back a challenge $E_{K_{pu}^A}(N_A \parallel N_{mcs})$ to the patient A using A's public key that has been certificated during Steps 1 and 2. This message also contains a timestamp from the MCS. This message can only be opened by the patient A. When the patient A has seen the nonce N_A inside, it has authenticated the MCS as only MCS has the access to the nonce.
- Step 5: Similar to Step 4, the MCS has authenticated the patient A.
- Step 6: Patient A sends a message $E_{K_{pu}^{mcs}}(E_{K_{pu}^A}(K_{contract}))$ to the MCS encrypted by using the MCS's public key and the patient A's private key. Encryption with the MCS's public key ensures that only MCS can open it. Encryption with the patient's private key ensures only patient A can create it. The contract cryptographic key is created which has authorized the MCS's access to the A's PHI data during this particular illness treatment process.

2) *PHI data generation and upload:* We split up the PHI data into two parts. (1) Part 1: Data_text consists of sensitive textual data including name, address, medical text results, etc. (2) Part 2: Data_image consists of large volume of data such as medical images, etc.

Those who are generating the PHI data must sign, encrypt and then send the data back to the MCS through the following internal uploading protocol as shown in Fig. 3. The retrieval of these data needs to go through the authentication security protocol as shown in Fig. 4.

For the ease of management, each personnel including medical doctors involved in dealing with patient PHI data needs to register with the MCS and is issued an internal e-health smartcard that contains the (private key, public key) pair. The medical care personnel, e.g, a doctor, needs to follow the internal authentication protocol as shown in Fig. 3 for uploading the patient A's PHI data to the MCS server. Message 1 is sent by the doctor requesting the permission for uploading the PHI data. The nonce of the doctor and the patient's ID are encrypted by the

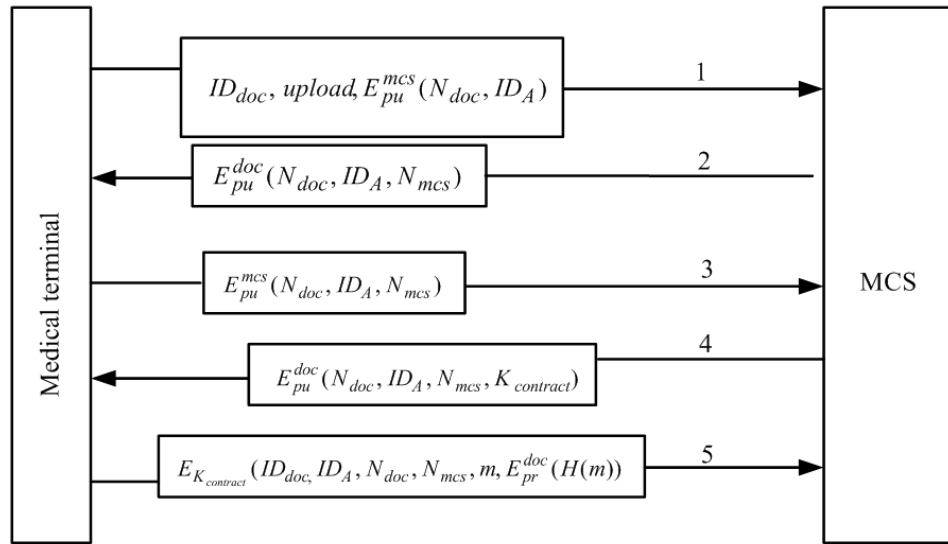


Fig. 3. Internal PHI data uploading protocol.

MCS’s public key which ensures that only MCS can open it. MCS also generates a nonce and sends the contract key. The message is encrypted using the doctor’s public key to ensure that only this doctor can open this message. When the doctor opens the message 2, it knows it is communicating with the MCS as only MCS can have access to the nonce N_{doc} . It also unlikely to have a reply attack as the nonce is a random large number which has been generated and sent milliseconds ago. For the same reason, message 3 allows the MCS to authenticate the doctor. Message 4 transmits the contract key of the patient to the doctor and message 5 is uploading the PHI data using symmetric encryption. This is for the efficiency purpose when the PHI data contains a large volume of image data $Data_image$. A signature from the doctor is attached on top of the hashed $Data_image$. If the PHI data m does not have a large volume of image data, we can upload the PHI data m encrypted using MCS’s public key and signed by the doctor’s private key.

C. Data Retrieval

During the contract period, we can use the following PHI data retrieval protocol as shown in Fig. 4. Messages 1 through 4 are for the purpose of mutual authentication and distribution of the secret contract key of the patient. The item $Retr(m)$ refers to PHI data that needs to be retrieved.

Similarly, the large volume of Data_image is encrypted using the symmetric cryptography for the efficiency purpose. If no large volume of PHI data Dat_image is involved, the system may choose to send the PHD data encrypted with the doctor's public key by merging messages 4 and 5.

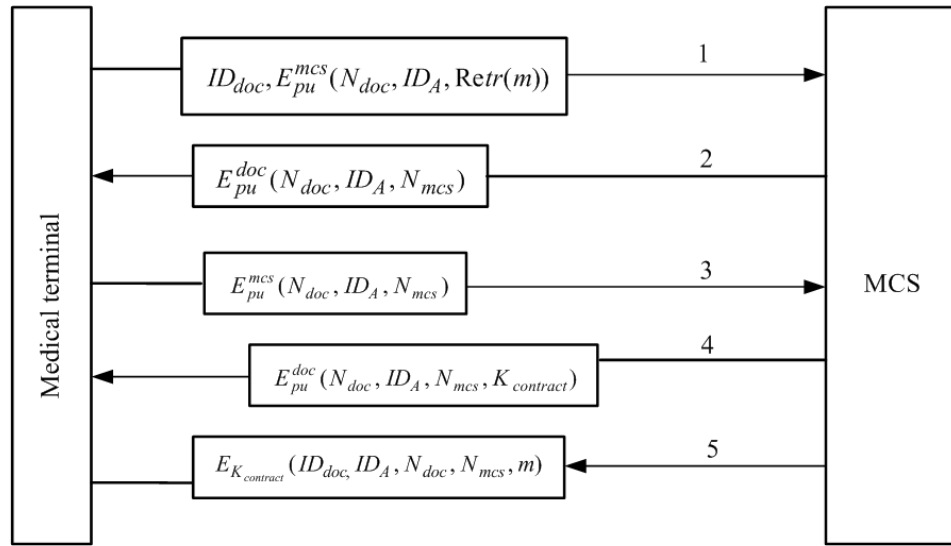


Fig. 4. PHI data retrieval protocol during contract period.

D. End of Contract

At the end of contract, the MCS will store the PHI data in the form of $[EDC, E_{K_{pu}^{mcs}}(H(EDC))]$ where we have $EDC = [E_{K_{contract}}(ID_{doc}, N_{doc}, N_{mcs}, PHI(Data_image), E_{pr}^{doc}(H(PHI(Data_image))))], K_{pu}^{doc}, E_{K_{pu}^A}(PHI(Data_text))]$. This data will be made a copy and delivered via secure channel to the patient A. Also, a message $E_{K_{pu}^{ste}}[PHI(Data_text), timestamp, E_{pr}^{mcs}(H(PHI(Data_text)))]$ is sent by the MCS to the STC for storage. A de-identification number is used to link the patient A and his/her EDC in the MCS. By contract, the MCS must destroy $PHI(Data_text)$ at this stage.

E. Next Cycle

For the next new medical care service, the patient will sign the new contract accordingly and provide his $PHI(Data_text)$ using his private key. The patient has an option to use previous contract key or create a new one. All other processes are the same as that of the first visit.

F. Mobility

Medical service providers must have formed a federated database. At the foreign MSC, the PHI data generation and access follow the same protocols as in the home MCS except when there is a need to get access to the home MCS. As shown in Fig. 5, the patient can provide his PHI(Data_text) to the foreign MCS and the contract key established between the patient and his home MCS for access to the home MCS. For stronger security, the foreign MCS and the home MCS need to go through similar authentication process before the contract key can be used for the access between foreign MCS and the home MCS.

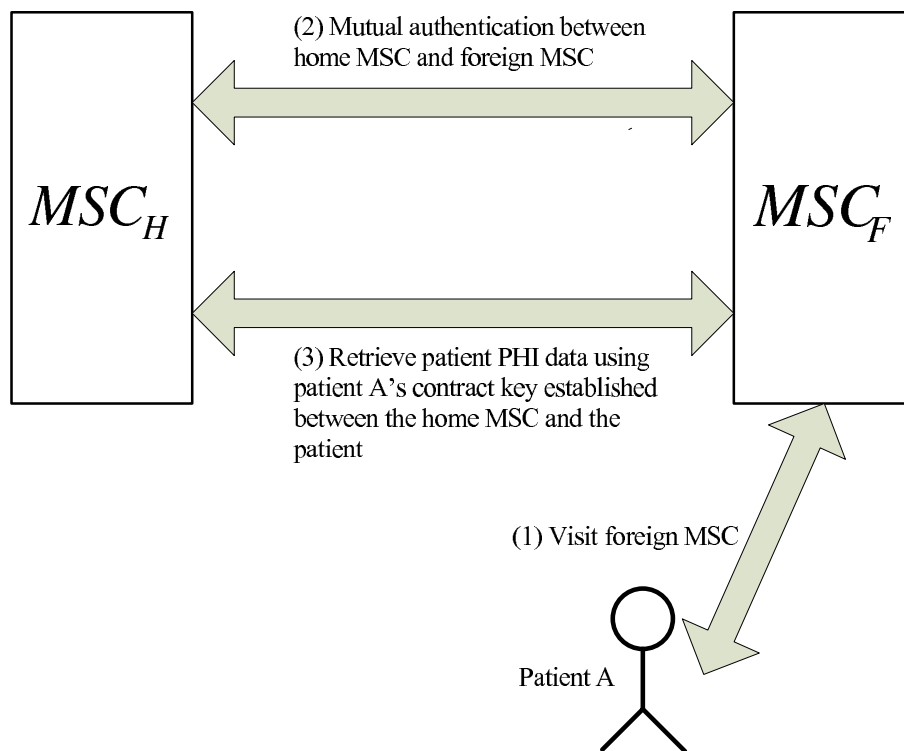


Fig. 5. Mobility process.

G. Emergency

In emergency cases, the medical service provider can retrieve the patient's PHI(Data_text) data after mutual authentication with the STC. It can also retrieve the rest data PHI(Data_image) after mutual authentication with the home MCS.

III. DISCUSSIONS

A. Compliance with HIPAA Regulations

1) *Patient's understanding*: At the very top level, a patient needs to sign the contract with both the STC and MCS governing the use of his PHI data.

Contract with STC: A patient needs to sign the contract with the STC when registering for the *e*-health smartcard. As the patient has to present in person, the contract can be done either in paper or electronically. The contract will set up the terms and regulations on how this *e*-health smartcard can be used. It also explains how his/her PHI data will be stored in the MCS and how it will be retrieved without his consent by the MCS in case of exemption.

Contract with MCS: A patient needs to sign the contract with the MCS when visiting the medical service provider. The patient has to be present in person, and the contract can be signed either in paper or electronic form [$E_{K_{pu}^A}(contract)$, $E_{K_{pu}^{mcs}}(contract)$]. The contract will set up the terms and regulations on how his/her PHI data will be accessed and stored according to the security protocols illustrated above. The patient will use his/her *e*-health smartcard to generate a contract key for the MCS to use.

The signed contract has provided the evidence that the patient understands how his/her PHI data will be used. It also serves as the evidence that the MCS has committed to follow the security protocols regarding PHI data generation, retrieval and exemption.

2) *Confidentiality*: The Contract Key Generation Protocol will ensure that a shared cryptographic key is securely generated by the patient and distributed to the MCS. All PHI data are either encrypted by this contract key or the patient's public to obtain confidentiality.

Although no encryption is suggested for the contract key stored in the MCS, the access to the key has to pass the medical service provider's internal authentication protocol (such as procedures 1 through 3 as shown in Figs. 3 and 4). The MCS issues its own internal PKI based *e*-health smartcard to its personnel who would need access to the patient PHI data. The PKI based authentication protocol discussed above can provide cryptographic security against unauthorized access to the PHI data. On top of this conventional PKI protection, this scheme can provide a better management for the secure access of the PHI data as the MCS has the best knowledge about its own organization including dynamic personnel update.

3) *Patient's control*: Access to the patient's PHI data is controlled by the patient's contract key. The major difference between our proposed scheme and the existing scheme [6] is that

we delegate the patient's cryptographic security control to the MCS during the contract period, while the latter requires the patient's physical presence each time an access is needed.

Several remarks can be made based on the above discussions.

- (a) Often it is infeasible for a patient to be physically present during the whole process of PHI data generation and analysis. For example, some test sample needs to be sent to another laboratory for processing and analysis. A doctor needs to have a meeting with other medical experts to discuss the case. It is therefore unrealistic to encrypt the PHI data using the patient's public key at the end of the outpatient service. The contract based scheme proposed in this paper has solved this problem by delegating the management to the medical service provider. The medical service provider has unlimited access to the generation and retrieval of the patient's PHI data during the contract period.
- (b) The cryptographic strength of the proposed patient's control scheme is as strong as the conventional symmetric cryptography if the MCS system is trusted. The proposed contract based scheme seems to be out of patient's control during the contract period as relevant medical service provider has unlimited access to the patient's PHI data without the patient's presence. However, this is just an illusion. The system is cryptographically strong against non-authorized personnel. For those who have legitimate access to the PHI data, no technology can prevent the confidentiality problem if they are not trusted. For example, a medical care personnel involved can write down a note even before presenting it to the patient.
- (c) For storage and transmission of a high volume of PHI data such as medical images, a symmetric encryption/decryption scheme is deployed using the contract key. This will enhance system efficiency significantly. Furthermore, the computing equipments such as desktop terminals are computing resource rich and also physically secure within the medical service provider organization. In [6], computing resource limited smartcard is required to do such a task which is infeasible.

4) *Data integrity*: Due to the authentication protocol and digital signatures deployed in the proposed scheme in the PHI data uploading and access, data integrity is ensured. As the PHI(Data_text) is signed and sent to the STC, even the MCS can not tamper the data after the contract expires. A copy of such data delivered to the patient can also add protection of data

integrity and data redundancy. We consider this component as optional though in the system as this data can get lost relatively easy by the patient. Again, there is a risk that the MCS does not destroy the PHI(Data_text) at the end of the contract. Our argument is that MCS has the capability to store the PHI(Data_text) during the process of the legitimate medical care service anyway no matter what technology is used. In our scheme, the commitment of security management by the MCS is bound by the legal contract where non-repudiation is ensured cryptographically after the end of the contract.

5) *Consent exception:* In the case of life-saving and other exceptional situations where the patient's authorization is not available, a MCS needs to go through a PKI mutual authentication protocol with the STC to get patient's PHI(Data_text).

IV. CONCLUSIONS AND FUTURE WORKS

In this paper, a hybrid public key infrastructure (HPKI) solution is proposed to address the HIPAA privacy and security regulations in *e*-health systems. Instead of adopting conventional session based cryptographic key management, our scheme is contract based. Within this contract period, the contracted medical service provider has unlimited access to the patient's PHI data under the condition that each access is controlled in terms of cryptographic authentication, encryption and non-repudiation, etc., by the medical service provider within its own organization. The delegation of patient's control to the medical service provider has avoided the problem of requesting a physical presence of the patient for each such access. This architecture is analogy to the current paper based health care system which is very beneficial to the real life implementation. The cryptographic strength of the system is as strong as the cryptographic strength of the cryptographic contract key. The proposed scheme can address the HIPAA privacy and security regulations.

To balance the needs of strong cryptographic security and efficiency performance, it is suggested to split up the PHI data into textual data part and image data part. For resource less demanding textual PHI data, we have the option of using strong PKI. While for resource demanding PHI image data, efficient symmetric cryptography is a must. Furthermore, a general digital mammogram is around 50 MB [16]. This will render it impossible to conduct encryption and decryption within a smartcard which was proposed in [6]. Even with efficient advanced

encryption standard (AES) scheme and powerful desktop PC, encryption of very high volume of digital medical images is still challenging and is an interesting topic for future research. Non-conventional encryption theory that is based on the features of medical images shows promising results [21].

Smartcard based authentication solutions have a fundamental weakness. That is, it can not authenticate the presenter of the token. The best they can achieve is to prove that the presenter has the right token and knowledge of the PIN (personal identification number) if the authentication protocol combines PIN. However, tokens can be lost and stolen. PIN can also be stolen and guessed out. Biometrics such as fingerprints can provide stronger authentication mechanisms [17][18]. Although many biometric authentication applications tend to embed biometrics such as fingerprint into the smartcard, it should be pointed out that the mobile biometrics template embedded in the smartcard runs a high risk of being comprised once the smartcard is stolen or lost. Recent research indicates that the fingerprint minutiae which can be used to recover the fingerprint [19]. Reliable mobile template protection is still an open issue [20][22]. It is preferred to use central matching scheme for the biometric authentication in *e*-health security systems due to the fact that it can avoid the issue of mobile template compromise and physically secure organizational infrastructure can offer better computing resources.

V. ACKNOWLEDGEMENTS

The authors would like to thank the financial support from the Australia Research Council (ARC) Linkage Project (LP0455324), ARC Discovery Project (DP0985838), and the National Science Council research grant (NSC97-2219-E-006-004), Taiwan.

REFERENCES

- [1] W. D. Yu and M. A. Chekhanovskiy, "An electronic health record content protection system using smartcard and PMR," The 9th International Conference on e-Health Networking, Application and Services, 19-22 June 2007, pp.11 - 18.
- [2] HIMSS Reports: "System interHIMSS Reports: "Systemic Interoperability Commission Releases Report to Congress and Administration", October 25, 2005, http://www.himss.org/ASP/topics_News_item.asp?cid=65448&tid=3. Retrieved on 28 January 2008.
- [3] W. D. Yu, P. Ray, T. Motoc. "A RFID technology based wireless mobile multimedia system in healthcare," The 8th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2006, 17-19 Aug 2006, pp.1 - 8.

- [4] R. Bhatti, A. Samuel, M. Y. Eltabakh, H. Amjad and A. Ghafoor, "Engineering a policy-based system for federated healthcare databases," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 19, No.3, Sept., 2007, pp.1288-1304.
- [5] T. T. May, "Medical information security: the evolving challenge," *IEEE* 1998, pp.85-92.
- [6] W. B. Lee, and C. D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no.1, Jan. 2008, pp.34-41.
- [7] "Standards for privacy of individually identifiable health information," *Fed. Regist.*, vol. 67, pp.53181-53273, 2002.
- [8] G. M. Stevens, "A brief summary of the medical privacy rule," *CRS Rep. Congr.* 2003.
- [9] A. Levi, M. U. Caglayan and C. K. Koc, "Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure," *ACM Transactions on Information and System Security*, Vol. 7, o. 1, Feb. 2004, pp.21-59.
- [10] P.A. Karger, "Privacy and security threat analysis of the federal employee personal identity verification (PIV) program," *Symposium on Usable Privacy and Security (SOUPS) 2006*, July 12-14, 2006, Pittsburg, PA, USA, pp.114-121.
- [11] J. S. Dwoskin, and R. B. Lee, "Hardware-rooted trust for secure key management and transient trust," *ACM CCS'07*, October 29-November, 2007, Alexandria, Virginia, USA, pp.389-400.
- [12] W. Stallings, "Cryptography and Network Security: Principles and Practices", International Edition, 3rd Edition, Practice Hall, 2003.
- [13] R. Agrawal, D. Asonov, R. Bayardo, T. Grandison, C. Johnson, and J. Kiernan, "Managing disclosure of private healthcare data with hippocratic database," *White paper, IBM*, Jan. 2005.
- [14] R. Agrawal and C. Johnson, "Securing electronic health records without impeding the flow of information," *Proc. International Medical Informatics Association Working Conference Security in Health Information Systems*, April 2006.
- [15] L. Alschuler, "Layered constraints: the proposal for HL7 healthcare templates," *XML*, 2002.
- [16] X. Q. Zhou, H. K. Huang and S. L. Lou, "Authenticity and integrity of digital mammography images," *IEEE Trans. On Medical Imaging*, vol.20, no.8, pp.784-791, 2001.
- [17] F. Han, J. Hu, X. Yu and Y. Wang, "Fingerprint images encryption via multi-scroll chaotic attractors," *Applied Mathematics and Computation*, Elsevier, Vol. 185, pp.931-939, 2007.
- [18] Y. Wang, J. Hu and D. Philip, "A fingerprint orientation model based on 2D Fourier Expansion (FOMFE) and its application to singular-point detection and fingerprint Indexing," *Special Issue on Biometrics: Progress and Directions, IEEE Transactions on Pattern Analysis and Machine Intelligence*, April 2007, vol. 29, no.4, pp.573-585.
- [19] A. Ross, J. Shah and A.K. Jain, "From template to image: reconstructing fingerprints from minutiae points," *Special Issue on Biometrics: Progress and Directions, IEEE Transactions on Pattern Analysis and Machine Intelligence*, April 2007, vol. 29, no.4, pp.544-560.
- [20] J. Hu, "Mobile fingerprint template protection: progress and open issues," *Invited Session on Pattern Analysis and Biometrics, the 3rd IEEE Conference on Industrial Electronics and Applications*, Singapore, 3-5 June, 2008.
- [21] J. Hu, F. Han, "A pixel-based scrambling scheme for digital medical images protection," *Journal of network and Computer applications*, Elsevier, 2009 (in press, doi:10.1016/j.jnca.2009.02.009).
- [22] K. Xi and J. Hu, "A New pre-alignment free fuzzy fingerprint vault using composite feature," *IEEE International Conference Communication (ICC)*, June 2009, Dresden, Germany (accepted, to be presented).