MEDINFO 2004
M. Fieschi et al. (Eds)
Amsterdam: IOS Press

Healthcare Public Key Infrastructure (HPKI) and Non-profit Organization (NPO): Essentials for Healthcare Data Exchange

Hiroshi Takeda[a], Yasushi Matsumura[a], Katsuhiko Nakagawa[a], Tadamasa Teratani[a], Zhang Qiyan[a], Hideo Kusuoka[b], Masami Matsuoka[c]

[a] *Department of Medical Information Science, Graduate School of Medicine, Osaka University ,Japan*
[b] *Osaka National Hospital, Japan*
[c] *Matsuoka Clinic, Japan*

Abstract

To share healthcare information and to promote cooperation among healthcare providers and customers (patients) under computerized network environment, a non-profit organization (NPO), named as OCHIS, was established at Osaka, Japan in 2003. Since security and confidentiality issues on the Internet have been major concerns in the OCHIS, the system has been based on healthcare public key infrastructure (HPKI), and found that there remained problems to be solved technically and operationally. An experimental study was conducted to elucidate the central and the local function in terms of a registration authority and a time stamp authority by contracting with the Ministry of Economics and Trading Industries in 2003. This paper describes the experimental design with NPO and the results of the study concerning message security and HPKI. The developed system has been operated practically in Osaka urban area.

Keywords

Internet, data exchange, authentication, time stamp; public key infrastructure (PKI).

Introduction

Long time operation of an integrated hospital information system [1] that features a picture archiving and communication system (PACS) [2] and an electronic patient record system (EPR) [3] in Osaka University Hospital has facilitated to deploy regional healthcare systems [4] in Osaka area. Under contract with the Japanese Medical Information Systems Organization (MEDIS) and the Ministry of Economics and Trading Industries, the OCHIS project was started in 2001 in order to exchange healthcare information such as letter-of-referrals among healthcare institutions and to operate an EPR system for clinics, based on the concept application service provider (ASP). The system configuration was a web-based client server system with regional IP network, a virtually closed network, operated by NTT Co. Ltd. A regional data center (RDC) has been developed to store XML formatted referrals and a series of application software modules has been developed to process the healthcare data with Web-technology.

As security issues have been a top priority in this project, OCHIS decided to apply PKI services. Some authorities such as a certificate authority (CA) have been set up in the RDC, and the network access has been made available with PKI cards in accordance with a private certificate policy.

The experimental system was successfully developed and evaluated in 2002. The results indicated that the EPR system by means of ASP was not efficient due to slow communication and unreliable quality of service. As a consequence full service of the EPR was postponed for a while. Since the referrals exchange system was very potent and welcomed by patients as well as physicians, the shift of the network infrastructure from regional IP network to the Internet was recommended for further extension of this application.

A NPO has been established in February 2003 to promote the healthcare network enterprise such as the regional healthcare data exchange, and has successfully shifted the network environment to the Internet. For developing nation-wide healthcare PKI, the NPO has contracted with MEDIS to study the feasibility of the root CA as a Trusted Third Party (TTP) and the time-stamp authority (TSA). The paper describes the developed system and the results of the feasibility study.

Methods

Outline of the OCHIS

To establish a secure healthcare network, the OCHIS has developed the Web technology-oriented client-server system, using HPKI. Characteristics are summarized as follows:

1. Authentication and access control to the servers by installing public key certificate in the IC card.
2. Setting up a local certificate authority
3. Issue and deployment of the public key certificate in the IC card as a private certificate authority
4. Management of the access right by using the attribute role certificate authority
5. XML formatted electronic signature by using IC card

XML electronic signature is given to MERIT-9 [5] (healthcare DTD in XML) defined referrals by using IC.

This enterprise is further expanding the model and its practical deployment in consideration of application of the Japanese Digital Signature Act in the healthcare field..

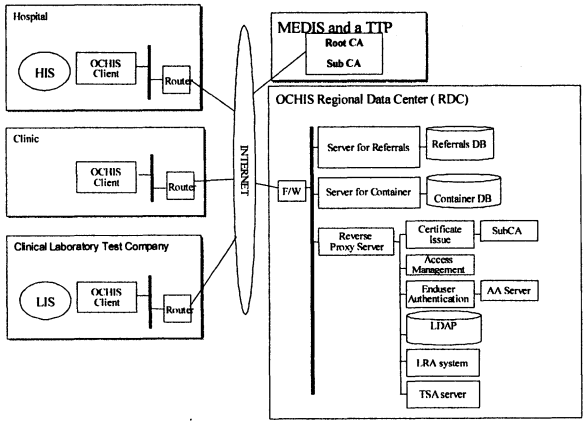

Figure 1 - System architecture of OCHIS for this study

Outline of the Experimental System

Sub-systems

The sub-systems that the OCHIS recently built within this enterprise are a LRA system, a local TSA system, an electronic signature system, and a multipurpose container system. The overall system architecture is illustrated in Figure 1

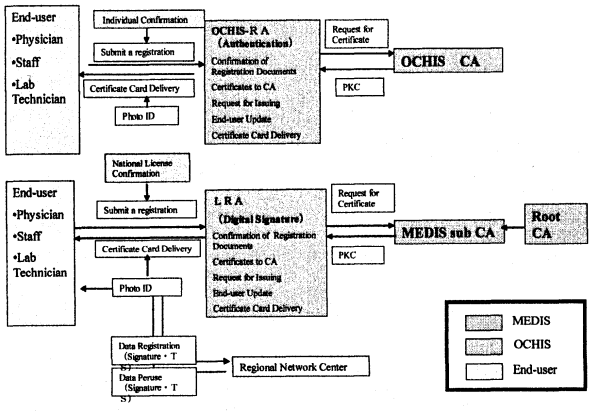

Figure 2 - Certificates issuing process in this study

1. LRA System

It is a system for registering authorized users in cooperation with a public CA that issues a public key certificate (PKC) and an attribute certificate (AC) in a IC card for electronic signature as a MEDIS Sub CA that is interlocked with the MEDIS RA (root authority). The method is basically based on X.509, RFC3280, RFC3281, ISO TS17090 and the Japanese Digital Signature Act [6].

2. Electronic Signature System

It is the system that performs XML formatted electronic signature with Time Stamp. The certificate for a signature is attached to referrals and clinical laboratory test result report data. The certificate policy (CP) and certificate performance statement(CPS) are based on MEDIS-|Healthcare PKI.

3. Multipurpose Container System

The system is able to give XML electronic signature to files with several records, possibly of different type such as clinical laboratory test report data. By using the container, a lot of healthcare data is transmitted at once with a single electronic signature.

4. Local TSA System

This is the system, which attaches a signature with time information to the hash value sent from the TSA client. The time information on Local TSA shall be acquired from the NTP server on the Internet. A time stamp request is periodically transmitted to MEDIS-TSA and the result is used to compare with those from the local TSA. The TSA system is designed to meet RFC3161.

Operation

As the Japanese guideline for PKI allows for an IC card to contain only one certificate, two types of IC cards should be issued at the OCHIS office for this experiment. The one is for authentication and the other is for digital signature. In conjunction with the root CA in MEDIS, a LRA in the office generates a key certificate for digital signature. Those keys are transported and handed to an end-user (end-entity) by a trusted courier service provider after identifying the person with a driver's license or a passport. The issuing process is summarized in Figure 2.

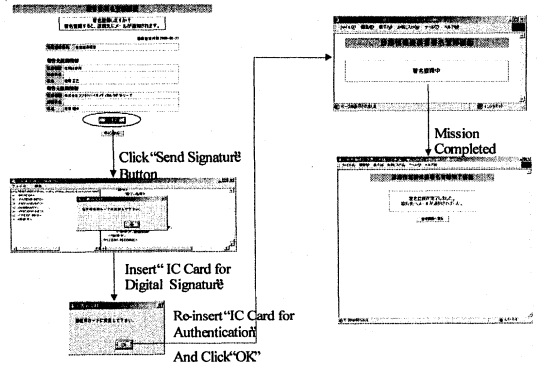

Figure 3 - Flow in attachment of a physician's digital signature to a letter-of-referrals

Two large-scale general hospitals have participated in this experimental study. For security reasons, hospitals are requested not to connect directly to the OCHIS network by the Internet but to install an OCHIS terminal at a Community Service Department in the hospital. In the Osaka University Hospital and National Osaka Hospital, by using the terminal at the Department, an authorized professional of the Department holds two IC cards to access the OCHIS network and to generate a digital signature one behalf of all doctors in the healthcare institution. Although it is basically requested to let a doctor's electronic signature on an electronic letter- of- referral by generated by himself, the huge number, more than one thousand, of doctors in educational institutions was expected to prevent smooth handling and maintenance of the IC cards, so a method of an institutional official digital signature has been adopted in this study.

For clinics, the OCHIS communication server is accessed by a doctor in a clinic with inserting his IC card for authentication. After his access right is reconfirmed, the letter-of-referral data and clinical laboratory test results for the doctor are retrieved via a Web server in the RDC. In case of generation of a new electronic letter -of- introduction or -referral to another doctor, the XML formatted electronic signature is attached using the IC card for the signature. In this experimental study, two kinds of IC cards (for authentication and for signature respectively) re utilized by a medical practitioner. The flow in attachment of a physician's digital signature is shown in Figure 3.

A clinical laboratory test company will produce so many test results reports a day that the transmission of those data is a critical mission in the company. The application of OCHIS is extended to those companies and an experiment concerning a container method and its security has been conducted. A company stores a set of the electronic laboratory test results in an electronic container with a digital signature of an authorized person and sends the container to a medical practitioner via the RDC of OCHIS. By using the container system with the functionality to attach XML electronic signatures to public documents it will also be applicable to other use cases than transportation of clinical laboratory test results.

In this experiment, the following healthcare providers have participated:

Two Hospitals (National Osaka Hospital and Osaka University Hospital), (One physician and one staff member at the department of community healthcare in each hospital were registered), ten Clinics, total ten medical practitioners were registered, one Clinical Laboratory Test Company (FUJIMOTOBAIO Medical Laboratories), Two Clinical laboratory technical engineers were registered.

Results

The issue of an IC card with public key certificate through LRA

The method for issuing the IC card for the electronic signature was designed. Digital data for PKC, AC, private key and distinguished name (DN) of the issuer and the user were recorded in the card in accordance with our Certificate Policy (CP). Each card was handed to the authorized user by using trusted courier service after the physical authentication was made by confirming with a face-photo ID on an public identification document. The role and function of the LRA was evaluated as effective in from security perspective.

End-entity authentication by using private key certificate

The evaluation of end-entity authentication indicates that the registration of end-entity and the issuing of public key certificate and private key by the private CA of the OCHIS should be logically the responsibility of two bodies. However, in the developmental phase of healthcare PKI, it will be acceptable to operate LRA and private CA in OCHIS RDC.

Transmission of healthcare data with digital signature

Letters-of-Referrals were generated on the Web- browser and the XML formatted digital signature was attached by using the private key stored in the IC card. In a clinic, the digital signature was made with using the medical practitioner's IC card. In a hospital, the XML-formatted signature of a doctor was endorsed with the digital signature in the IC card of the Community Service Department staff. The operation and the procedure in a hospital are based on a conventional operation, in which a paper letter-of-referral has been authorized with the official stamp of the hospital.

Reports of the laboratory test results were transmitted with a method of multi-purpose container and digital signature. Although it would be ideal to attach the digital signature of the authorized person of the test laboratory to each report, this would take time to do. Our method was evaluated as secure and practically useful and will be extended to other applications.

Electronic signature verification experiment

The electronic signature of a medical practitioner that was issued by the authorized CA (sub CA) was experimentally verified with the root CA in the MEDIS. The role as a physician was confirmed by matching with the central registry of medical license. Our electronic signature was further tested as effective by mutual verification with the XML formatted electronic signature of an other local project (the Itabashi central hospital) registered as another MEDIS sub CA. However, the question of validity of electronic signatures generated by the hospital staff and the clinical laboratory staff has been unresolved due to unclearness of the present regulations in Japan.

Local Time Stamp attachment

Time Stamp data were experimentally attached to letters-of-referrals and reports of laboratory test results. In the experiment, the stronger integrity of the electronic signature with time information was confirmed in terms of high encryption nature of letters-of-referrals.

Local TSA verification

Verification of the local time stamp was attested by linking regularly to MEDIS-TSA with local TSA. The usability of local Time Stamp was proved as a time proof by verification of the time stamp response of MEDIS-TSA and Local TSA.

Discussion

In today's IT driven health care environment, healthcare providers, healthcare organizations and partners should avoid from the vulnerability of electronic messages to interception and tampering when sent over unsecured channels such as the Internet. It is critical for custodians of healthcare information to establish and maintain the highest level of patient/consumer confidence in the process. Public Key Infrastructure (PKI) services are the solution of choice for shared encryption/decryption, digital signature, and authentication services. These services can be used in a variety of settings, including web-enabled patient and clinical information services [8] [9].

Major purpose of the study is to elucidate the functional differentiation between public Certificate Authority (CA) and private CA as a TTP (Trusted Third Party), and to establish a local time-stamp authority (TSA). Lessons learned from the study are categorized into points-of-view of end-users, NPO and healthcare PKI (HPKI).

Although two functions (authentication and signature) in two IC cards were required by Japanese guideline for PKI, it would be executed with single cards as a case of single sign on in the near future. In the experimental study, doctors in a hospital did not carry their cards for authentication and digital signature but a staff in the community healthcare liaison office made a physician's role as an Institution's Digital Signature. Acceptance and validation for the signature should be discussed in Japan.

One of major concerns in PKI is financial issue. Initial and maintenance cost for PKI operations such as policy development, application software, certificate publication, end user training and key management should be clearly open to public. Evaluation for security cost should be needed in the next step.

Reliance on the NPO is also key issue. Relying party must explicitly manage trust decisions. Trust would be business decision with business and legal consequences and robust business reliance infrastructure is not considered as "for free".

In HPKI point of view, interoperability of all certificates is the top priority. We must answer the following questions. Should all CA be required to implement common practices? While every healthcare provider may require a certificate for authentication, how is the healthcare staff signing authority restricted?

Persistence is another important issue. Since signed electronic documents have long retention periods, policy persistence should be needed. As signature verification must be possible for full document retention period, mechanisms to ensure availability of certificate and status information should be retained. For approaches to mitigate against technology advances that make it possible to discover the private key, persistence of private key protection would be technologically considered.

To cope with those lessons, medical informatics community must lead to develop and publish a Model Policy for the Healthcare Community of Interest, containing appropriate levels of assurance. And existing healthcare security providers are expected to encourage the use of these descriptions in Certificate Policy and Certification Practice Statements [10], and incorporate these descriptions into global regulations governing HPKI use.

Patients' participation will be the goal for healthcare data exchange [11]. Since so many hospitals, clinics and patients will communicate each other in an urban area, an NPO with HPKI will be an optimum solution for establishing an Internet data center.

Conclusion

Although Public key infrastructure (PKI) technology is a robust and proven solution for protecting electronic messages communicated over public networks, a few studies have been reported in healthcare field. The lessons learned in this study will provide an evidence for developing, establishing and deploying future global security systems in healthcare community. It is also emphasized that a non-profit organization (NPO) as a trusted third party should operate an Internet data center for healthcare data communications since the organization is neutral to national/regional government, healthcare providers, and customers/patients.

Acknowledgements

This study has been supported by Research for the Future program of Japan Society for the Promotion of Science (JSPS-RFTF 99I00905), grants-in-aid for scientific research of the Ministry of Labor, Health and welfare (No. H13-Iryou-019, H14-Iryou-006, H14- Iryou -016). Authors express sincere thanks to Mr. Hiroshi Oshima, Kouji Matusnami, Masataka Wanigawa for their great efforts for assistance.

References

[1] Y. Matsumura, H. Takeda and M. Inoue. Implementation of the totally integrated hospital information system (HUMANE) in Osaka University Hospital. In R.Greenes et al (Eds). *Proc. MEDINFO95*, pp 590-593, 1995.

[2] K.Inamura, J.Konishi, H. Nishitani, S. Kousaka, Y. Matsumura, H.Takeda , H.Kondoh: Status of PACS and technology assessment in Japan: *Computer Methods and Programs in Biomedicine* 66: 5-15,2001.

[3] Y. Matsumura, S. Kuwata, H. Kusuoka, Y. Takahashi, H. Onishi, T. Kawamoto and H. Takeda.. Dynamic viewer of medical events in electronic patient record. In V. Patel et al. (Eds). Proc. *MEDINFO2001*, pp.648-652, 2001.

[4] H.Takeda, Y. Matsumura, S. Kuwata, H. Nakano, N. Sakamoto, R.Yamamoto: Architecture for networked electronic patient record systems. *International Journal of Medical Informatics*. 60(2): 161-167,2000.

[5] http://merit-9.mi.hama-med.ac.jp/index-e.html

[6] http://www.meti.go.jp/english/report/data/gesignline.html

[7] G.. Kelly, B. McKenzie. Security, privacy, and confidentiality issues on the Internet. *J Med Internet Res* 4(2): e12, 2002.

[8] G..Pangalos, I.Mavridis, C. Ilioudis, C. Georgiadis. Developing a public key infrastructure for a secure regional e-Health environment. *Methods Inf Med.* 41(5):414-418, 2002.

[9] R. Brandner, M. van der Haak, M. Hartman, R. Haux, P. Schmucker. Electronic signature for medical documents--integration and evaluation of a public key infrastructure in hospitals. *Methods Inf Med.* 41(4):321-330, 2002.

[10]http://www.europki.org/ca/root/cps/en_index.html

[11]H. Takeda, H. Endoh. Commentary on 'Health care in the information society. A prognosis for the year 2013'. *International Journal of Medical Informatics.* 66(1-3): 107-111,2002.

Address for correspondence

Hiroshi Takeda, M.D., Ph.D

Department of Medical Information Science, Graduate School of Medicine, Osaka University, 2-15, Yamada-Oka, Suita 565-0871, Japan

E-mail: takeda@hp-info.med.osaka-u.ac.jp