Healthcare Information Systems Using Digital Signature and Synchronized Smart Cards via the Internet

Won Jay SONG* & Byung Ha AHN* & Won Hee KIM**

** Systems Engineering and Operations Research Labs, Department of Mechatronics, KwangJu Institute of Science and Technology, 500-712, Republic of Korea*
Tel: +82-62-970-2426, Fax: +82-62-970-2384, Email: wjsong@kjist.ac.kr & bayhay@kjist.ac.kr
*** VLSI and CAD Labs, Department of Electronics Engineering, Chungnam National University, 305-764, Republic of Korea*
Tel: +82-42-821-7707, Fax: +82-42-823-5436, Email: kimwonhee@empal.com

Abstract

This research paper presents a new 2-way double-type smartcard terminal's and a new system's design and development of the prescription order communication system (POCS) based on the Internet between the hospital and the pharmacy, on the public-key infrastructure (PKI), and on the concurrently parallel co-operation with both medical professional's and patient's smart cards in the 2-way double-type terminal under the synchronized status, in order to control security and privacy of patients and to manage drug histories of them. Concurrently parallel co-operation method at the synchronized status has been proposed in order to merge the digital signature generated by a medical professional with a patient's prescription data, to control security and privacy of patients, and to manage drug histories of them. The digital signatures written by the medical professionals (doctors and pharmacists) holding and using their individually master smart cards are applied to all contents of the prescription stored on a patient's slave smart card at the synchronized status in the 2-way double-type terminal. Therefore, digital signatures for all prescriptions stored on the smart card should effectively be used to prevent being altered, forged, and reused by unauthorized users and being repudiated by medical professionals.

1 Introduction

The traditional process in order to transfer a medical prescription from the hospital (or clinic) to the pharmacy is the paper-based communication using a prescription paper sheet with the doctor's real signature, which paper was prepared by a medical doctor for own authentification in a healthcare center.

A appropriately medical prescription is written out on the papers by a medical doctor after the doctor medically examines a patient to visit a healthcare center. Finally, the doctor signs and seals a prescription document in order to prevent being altered, forged, and reused by unauthorized users and being repudiated by medical professionals.

Disregarding a doctor's signature, paper-based medical' prescriptions should easily be duplicated, edited, and modified by one due to the help of advanced skills for the paper material reprint such as image scanners and color copy-machines. That illegal process will result medicinal abuse and make a serious trouble of promotion of the nation's health. The paper-based workflow between the hospital and the pharmacy should also be inefficient and produce unnecessary cost.

In recent, due to influence of the e-business, a wide variety of application of the Internet to the healthcare information systems has been introduced and various pilot researches and developments or tests have been implemented. The client/sever- and web-based healthcare information systems via the Internet have been applied to the new e-business solutions such as the enterprise resource planning (ERP) between medical professionals in a medical center, the customer relationship management (CRM) between medical professionals and patients, and the supply chain management (SCM) between a medical center and a pharmaceutical manufacturer. These new trials and attempts should be greatly efficient and successful for a viewpoint of the on-line workflow based on the networking between the hospital and the pharmacy, between the healthcare center and the manufacturer, or among all departments in a healthcare center. However, advanced researches are needed to improve another efficiency and solve serious problems of privacy and management of drug history for patients, security for medical professionals, and unpredictable disconnection of the Internet such as the off-line status.

In addition, smart cards have been understood as a key technology in the e-business era [1]-[3]. A few years ago, smart cards have been applied to the wide area of healthcare information systems in order to control medical professional's accesses to various application programs with graphic user interface (GUI) under the client/server computing environment via a local area network (LAN). However, until recent, smart cards have only been used as management tool of patient's drug and medical histories without concurrently parallel co-operations with any medical professional's smart card under the asynchronized status.

Therefore, this research paper proposes a new 2-way double-type smartcard terminal's and a new system's design and development of the POCS based on the Internet between the hospital and the pharmacy, on the PKI, and on the concurrently parallel co-operation with both medical professional's and patient's smart cards in the developed 2-way double-type terminal under the synchronized status. And then we will implement the proposed system using the developed terminals for "The government project for the separation of the dispensary from the doctors office in the Republic of Korea."

2 Characteristics of Related Systems

2.1 Smartcard-Based Healthcare Information Systems

Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'02)
0-7695-1506-1/02 $17.00 © 2002 IEEE

Physically, a smart card resembles a credit card having one or more semiconductor devices attached to a module embedded in the card's top left corner. The semiconductor device used in the smart cards contains a CPU and blocks of memory including RAM, ROM, and EEP-ROM [2].

Functionally, smart cards have two main advantages over magnetic-stripe cards. They can carry 10~100 times as much information and hold it more robustly and securely than do typical magnetic-stripe cards [3]. The smart card's ability to store and manipulate information or data can be used in a wide variety of healthcare applications for both private and authentication.

Healthcare applications provide an extremely important applications area for smart cards, that may also make the most important implementation of this technology, by improving patients' health and by saving patients' lives. For three examples of using smart cards as following that:

- Firstly, kidney patients in France and Japan can carry medical cards that hold their dialysis records and treatment prescriptions [3].
- Secondly, France and Sweden are also conducting pilot programs in which current records of prescription drug use will be maintained on smart cards [3].
- Thirdly, in recent, the health passport project have been going on at the first phase to 2001 years in the USA [http://www.westgov.org/wga/initiatives/hpp/].

Many peoples practically take multiple prescription drugs, for different conditions, possibly prescribed by different doctors, and filled by different pharmacies at different times. Smart card records can only alert the pharmacist, doctor, or user of adverse drug interactions [3].

Currently existing health applications using smart cards can not only carry individual's vital medical information and but also provide basic medical information as following that:

- Lists of unique individual drug sensitivities,
- Current conditions being treated,
- The name and phone number of a patient's doctor, and
- Other information vital in an emergency.

Another application is a secure collaborative telemedicine system using smart cards. The authentication services of the collaborative system support measures to restrict access to authenticated and authorized medical user holding the smart card in which an individual user's private keys and digital certificates of the public keys are stored. The patient cards only contain patient demographics, insurance information, clinical information, and medical emergency data. Healthcare professional cards simply include the personal identification number (PIN), a individual's private keys, and digital certificates of the public keys in order to access to the collaborative healthcare systems [4]. Authentificated process using these keys enable medical professionals to use at any point of collaborative care systems.

2.2 Network-Based Healthcare Information Systems

Traditionally, video conference systems, pagers, fax machines, and phones have been applied to overcome the distance and communication barrier between healthcare collaborators or related healthcare departments. Network-supported collaboration can also overcome the traditional distance barrier to healthcare by enabling communications between participants and easily and rapidly can access to information [4].

There is growing interest in the use of the world wide web (WWW) of the Internet- and Intranet-based client/server environment for delivering patient health status and related wellness information to medical professionals. Recently, medical centers are experimentally using the WWW server and browser clients via the Internet/Intranet to make a wide variety of information available to their professionals with related user ID and its password in front of the network-based client PC.

The advent of computer- and network-based patient records, the fast growth of electronic mail, and the Internet-based applications and resources such as the WWW have greatly improved productivity as a result of improved collaborative workflow for medical healthcare centers.

For maximum platform-independence and minimum collaborative workflow complexity, the 3-tier model has been applied [5]. Healthcare professionals using their user ID and their password in front of any networked PC on the client-tier could share collections of patient-related data on the server-tier that have different formats and origins using standardized remote retrieval and presentation tools. Medical data transmission should be initiated by a client application at the professional user's site which also could maintain visualization and manipulation of the received multimedia data such as X-ray and MRI images. A server application on the middle-tier would act as an interface to the database and deliver the requested data via TCP/IP over the Internet/Intranet.

Many regions in Europe develop experiences in order to improve the continuity of care by networking hospitals and general practitioners (GPs) [6]. If medical information is available within the hospital, it should be shared with other healthcare workers. The co-operation and collaboration of the healthcare workers can be supported by the network-based information systems as these systems include the telematics aspects [7]. If communication is essential between the different medical or non-medical units within an hospital, this communication becomes more and more indispensable with the external world: other hospitals, private clinics, GPs offices [8].

2.3 PKC-Based Healthcare Information Systems

The evolutionary development from traditionally paper-based to currently network-based patient record systems in a healthcare information system including database systems changes the research and development directions, in which we should deal with the patients' and medical professionals' privacy and security issues remarkably carefully [9].

Within the healthcare information system, there is an emerging need to insure the security and integrity of healthcare data while maintaining the patients' privacy [9]. The security of the care system is a greatly important point as confidentiality of medical and administrative information is one of the most important conditions for the use of telematics of healthcare [6].

General security requirement specifications in healthcare information systems practically are two securities in the database information and in the distributed- and network-based systems information [9]. Cryptography is taking a plain text and then encoding it to a ciphertext. Communications use cryptography should be useful and secure only to the sender and the related

receiver [10]. All modern cryptography schemes rely on the concept of keys.

Therefore, cryptography is a very important part to achieve secure communication and storage in database- and network-based medical information systems. It can help prevent intrusion from the outside. It can also protect privacy of users of the systems so that only authorized participants can comprehend communications.

A secret-key cryptographic system such as DES and AES is that the sender and the receiver know a shared single secret key [10]. The problem with using a secret key is transferring the secret key between the sender and the receiver using any secure communication channel without being eavesdropped by a wiretapper. However, that operating speed is so faster.

Another approach to solve this serious problem is the public-key cryptographic system such as RSA and ECC in which a message can be encrypted using one key and be decrypted using another key [10], i.e., all patient-related medical data encrypted using the private key can be decrypted using the public key and vice versa in the healthcare system. The public-key cryptography (PKC) is used for solving both privacy and authentication problems in the healthcare systems. However, that operating speed is slower than DES and AES.

In order to maximize information security and minimize time cost in healthcare environment, the plain medical text needs to be encrypted using a random secret-key generated by the sender's secret-key cryptographic system such as DES and AES. And then the random secret key itself will be encrypted using the public key generated by the receiver's public-key cryptographic system such as RSA and ECC. Finally, both the ciphertext and the encrypted secret key will be transmitted to the receiver via TCP/IP over the Internet. This approach combines the advantages of both secret- and public-key mechanisms.

Several network protocols are also available which use the combination of the secret- and public-key cryptographic systems. The secure HTTP and secure socket layer (SSL) protocols of a wide variety of protocols are the mostly used protocol for the WWW applications.

3 Existing Systems' Problems and Models in the Republic of Korea

3.1 Currently Existing Systems' Problems

Currently existing healthcare information systems using smartcard-, network-, and PKC-based workflows should imply serious demerits as following that:

- In the smartcard-based system, information and data with respect to the relation between medical professionals and patients do not store on the patient's smart card. It means that medical prescription data (with respect to a patient) written by a professional only store on the patient's card.
- In the network- and smartcard-based systems, a professional's smart card is only used in accessing to application programs in network-based client/server systems. Also, all medical prescription data exception of relation information between a medical professional and a patient only store on the patient's smart card.
- In the PKC- and smartcard-based systems, PINs and private keys of all medical professionals (who would like to access to securely collaborative healthcare information systems) are extremely important, and then each PIN and private key should be stored on each professional's individual smartcard. i.e., the card with a private key is only used in generation of login and access data.

From the above facts, relation-oriented data and information between medical professionals and patients such as the digital signatures and the digital certificates need to be stored on the patients' and the professionals' smart cards under smartcard-, network-, and PKC-based fusion environments, respectively. And that scheme is most important in order to promote the nation's health.

Due to the effect of the e-business, the network-based healthcare information systems should be most important and be developed in accordance with the following three essential points:

1. The Internet/Intranet will be closely interconnected to make obvious for the physical location of the patient's data, processing, and services;
2. The services and applications available on the both networks will have to offer great interoperability in order to provide the user with enhanced comfort of use and greater possibilities for the treatment and linking of the distributed patient's data; and
3. The communication between server and clients via the Internet/Intranet should be secured by cryptographic techniques such as the secure HTTP or the secure socket layer (SSL).

Therefore, for "The government project for the separation of the dispensary from the doctors office in the Republic of Korea," we propose a new system design and will implement it, in which a patient's prescription data merged with a professional's digital signature have been stored on the patient's smart card under the network- and PKC-based environments. Concurrently parallel co-operation method at the synchronized status is proposed in order to merge the digital signature generated by a medical professional with a patient's prescription data.

3.2 Currently Existing Systems' Problems

We have classified and analyzed the new models of the prescription order communication system (POCS) in the Republic of Korea into four types as following that:

1. POCS using the Internet,
2. POCS using the 2-dimensional bar code,
3. POCS using the kiosk, and
4. POCS using the smart card.

And the major functions have been considered as following that:

- Patient's medical privacy and drug history,
- Reservation of the prescription from a hospital and a pharmacy,
- Renunciation of the reserved prescription,
- Information of the pharmacy (location, drug, and etc.), and
- Medical fee.

The POCS using the kiosk or the 2-dimensional bar code is relatively simple and similar to the POCS using the paper-based workflow. The best universal and reliable concept of reservation for the prescription will be the Internet in the status of on-line. The POCS using the smart card will not only play a important role in order to manage a patient's drug and medical histories and but also transfer a patient's prescription on a smart card from a hospital to a pharmacy in the status of off-line. Therefore, we will use both the Internet and the smart card for on-line and off-line, respectively.

4 Proposed System's Design and Development

4.1 System Design and Its Components

Proposed healthcare information system is redesigned as following subsystems in Figure 1:

- One WWW-based remote server system in order to authenticate, certificate, and authorize,
- Two WWW-based local server systems in the hospital and the pharmacy, respectively,
- Three browser-based local client systems in the hospital and the pharmacy, respectively, and
- the Internet.

Securely external communication channel between the hospital and the pharmacy is used via secure HTTP over the Internet. Securely internal communication channel for all department in the hospital or the pharmacy is also used via secure HTTP over the Intranet as shown in Figure 2.

Four 2-way type smartcard terminals are installed at four browser-based clients of six clients as shown in Figure 1. The terminal includes two smartcard readers for a medical professional and a patient within one body as shown in Figure 3. Its terminal regularly operates only at the synchronized status when both a medical professional's and a patient's smart cards are concurrently parallel inserted at the terminal.

4.2 Prototype System Development and Its Functions

The proposed system is development of a prototype system using computer software languages as following that:

- Microsoft SQL, ASP, and VBScript,
- Microsoft Visual C++ in order to connect between a terminal and a PC, and
- Microsoft CryptoAPI in order to generate private and public keys and digital signatures.

The proposed system presents a secure transmission of a patient's medical prescription from the hospital (or clinic) to the pharmacy via the Internet/Intranet and the concurrently parallel co-operation with both patient's and professional's smart cards in the 2-way type terminal under the synchronized status as shown in Figure 1.

The secure Internet/Intranet and smart card terminals consist of all computer machines in the hospital (or clinic) and the pharmacy over the secure HTTP or SSL protocols based on TCP/IP, respectively, as shown in Figure 2.

In the developed prototype system and terminal, the digital signatures written by the medical professionals (doctors and pharmacists) holding and using their individually master smart cards are applied to all contents of the prescription stored on a patient's slave smart card at the synchronized status. Therefore, digital signatures for all prescriptions stored on the smart card should effectively be used to prevent being altered, forged, and reused by unauthorized users and being repudiated by medical professionals as shown in Figure 4.

In addition, all medical professionals need to own individually their master smart card within:

- the private key for generation of the digital signature,
- the digital certificate issued from the certification or registration authority for the professional's public key, and
- the public key of the authority

as shown at the left- and right-top in Figure 4.

In order to operate the developed prototype system, the private and public keys will be stored on the medical professional's master smart card in the hospital (or clinic) and the pharmacy. i.e., that keys are issued at the Intranet local server in the hospital or the pharmacy, and then the keys are stored on the card. The stored private key should be encrypted using the DES (Data Encryption Standard) algorithm and PIN installed in the microprocess on the smart card. The generated public key should be registered at the remote management server through the secure Internet communication channel such as secure HTTP or SSL protocols. The individually digital certificate for the registered public key is issued and transferred to the public key's owner over the secure Internet communication channel as shown at the center in Figure 4.

In order to make relation-oriented data and information between a professional and a patient, a digital signature is created by running a patient's prescription message through a hashing algorithm. This yields a message digest, i.e., a condensed version of the original prescription text. The message digest is encrypted using the private key of the medical professional, turing it into a digital signature. In the developed prototype system, a medical professional's digital signature should be relation-oriented information created using a patient's medical prescription data on the slave smart card and the professional's private key on the master smart card in the 2-way type terminal under the synchronized status. The digital signature should provide prescription authentication, non-repudiation of origin, and medical data integrity. The digital signature can only be verified using the public key of the same medical professional. The receiver of the message decrypts the digital signature and compares the result with a message digest recalculated from the original message text. If the two are identical, the message has not been manipulated. It is authentic.

4.3 Proposed System's Improvement over Existing Systems

The paper-based systems, disregarding a doctor's written signature, should easily be duplicated, edited, and modified by one due to the help of advanced skills for the paper material reprint such as image scanners and color copy-machines. That illegal process will result medicinal abuse and make a serious trouble of promotion of the nation's health. The paper-based workflow between the hospital and the pharmacy should also be inefficient and produc unnecessary cost.

The network-based systems should be greatly efficient and successful for a viewpoint of the on-line workflow based on the networking between the hospital and the pharmacy or among all departments in a healthcare center. However, advanced improvements are needed to add another efficiency and solve serious problems of privacy and management of drug history for patients, security for medical professionals, and unpredictable disconnection of the Internet such as the off-line status.

The smartcard-based systems should control medical professional's accesses to various application programs with graphic user interface (GUI) under the client/server computing environment via a local area network (LAN). In addition, until recent, smart cards have only been used as management tool of patient's drug and medical histories without concurrently parallel co-operations with any medical professional's smart card under the asynchronized status.

The proposed system employs the Internet between the hospital and the pharmacy, the public-key infrastructure (PKI), and the concurrently parallel co-operation with both medical professional's and patient's smart cards in the 2-way type terminal under the synchronized status to

the currently existing healthcare information systems. In the developed prototype system and terminal, the digital signatures written by the medical professionals (doctors and pharmacists) holding and using their individually master smart cards are applied to all contents of the prescription stored on a patient's slave smart card at the synchronized status. Therefore, digital signatures for all prescriptions stored on the smart card should effectively be used to prevent being altered, forged, and reused by unauthorized users and being repudiated by medical professionals. In addition, given professional's (master) and patient's (slave) smart cards inserted into the 2-way double-type smartcard terminal, the developed prototype system should provide higher efficiency and enhanced security rather than currently existing healthcare information systems in the Republic of Korea.

5 Conclusions and Further Studies

In recent, due to influence of the e-business, a wide variety of application of the Internet to the healthcare information systems should be greatly efficient and successful for a viewpoint of the on-line workflow based on the networking between the hospital and the pharmacy, between the medical center and the manufacturer, or among all departments in a healthcare center. However, although the employment of the e-business via the Internet has been successful in medical and healthcare centers, more advanced researches are needed to improve another efficiency and solve serious problems of privacy and management of drug history for patients, security for medical professionals, and unpredictable disconnection of the Internet such as the off-line status.

We have classified and analyzed the currently existing smartcard-, network-, and PKI-based healthcare information systems [4]-[10]. Through the classification and analysis, relation-oriented data and information between medical professionals and patients such as the digital signature and the digital certificate need to be stored on the patients' smart cards under smartcard-, network-, and PKI-based fusion environments. We have also classified and analyzed the models of the POCS in the Republic of Korea into four types toward the ideal model. Four candidate models of the POCS indicate that if the Internet and the smart card will be merged, then those will cover all major functions of the POCS.

Therefore, this research paper proposes a new 2-way double-type smartcard terminal's and a new system's design and development of the POCS based on the Internet between the hospital and the pharmacy, on the PKI, and on the concurrently parallel co-operation with both medical professional's and patient's smart cards in the developed 2-way double-type terminal under the synchronized status, in order to control security and privacy of patients and to manage drug histories of them. And then we will implement the proposed system using the developed terminals for "The government project for the separation of the dispensary from the doctors office in the Republic of Korea."

A patient's prescription data merged with a professional's digital signature in the developed smartcard terminal have been stored on the patient's smart card under the network- and PKI-based fusion environments. Concurrently parallel co-operation method at the synchronized status has been proposed in order to merge the digital signature generated by a medical professional with a patient's prescription data, to control security and privacy of patients, and to manage drug histories of them.

Therefore, the proposed system should feature the secure transmission of a patient's medical prescription from the hospital to the pharmacy via the Internet/Intranet under the on-line status and the concurrently parallel co-operation with both patient's and professional's smart cards in the 2-way double-type terminal under the synchronized status.

In the developed prototype system and terminal, the digital signatures written by the medical professionals (doctors and pharmacists) holding and using their individually master smart cards are applied to all contents of the prescription stored on a patient's slave smart card at the synchronized status. Therefore, digital signatures for all prescriptions stored on the smart card should effectively be used to prevent being altered, forged, and reused by unauthorized users and being repudiated by medical professionals.

Given professional's (master) and patient's (slave) smart cards inserted into the 2-way double-type smartcard terminal, the developed prototype system should provide higher efficiency and enhanced security rather than currently existing healthcare information systems in the Republic of Korea. And then personal healthcare information should also be protected on the smart card.

In addition, the smartcard-based electronic payment system (electronic purse) for POCS needs to be studied in order to improve the payment workflow from the traditional model to the currently modern e-commerce model.

References

[1] F.Seliger and U.Steinmueller, "Accessing smart cards using Java," The IBM Technical Developer Conference, 1999.

[2] C.H.Fancher, "In your pocket: smartcards," IEEE Spectrum, Vol.34, No.2, 1997.

[3] J.J.Farrell III, "Smartcards become an international technology," TRON Project International Symposium, 1996.

[4] R.S.Raman, V.Jagannathan, R.Reddy, "Secure collaboration technology for healthcare enterprises," IEEE Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1997.

[5] M.Back, T.Norgall, M.Rommel, C.Zywietz, "Internet/Intranet access to a multimedia cardiology information system," Computers in Cardiology, 1999.

[6] R.J.Beuscart, D.Delerue, A.Souf, "A regional information network: management and security," International Conference of the IEEE Engineering in Medicine and Biology Society, 1998.

[7] R.Beuscart, J.-M.Renard, D.Delerue, A.Souf, "Telecommunication in healthcare for a better coordination between hospitals and GP's: routine application of the 'ISAR-Telematics' project," IEEE Transactions on Information Technology in Biomedicine, Vol.3, No.2, 1999.

[8] T.P.Clemmer, "The role of medical informatics in telemedicine," Journal of Medical Systems, Vol.19, No.1, 1995.

[9] Y.Y.Al-Salqan, "Security and confidentiality in healthcare," IEEE International Workshops on informatics Enabling Technologies: Infrastructure for Collaborative Enterprises, 1998.

[10] A.Menezes, P.Oorschot, and S.Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.

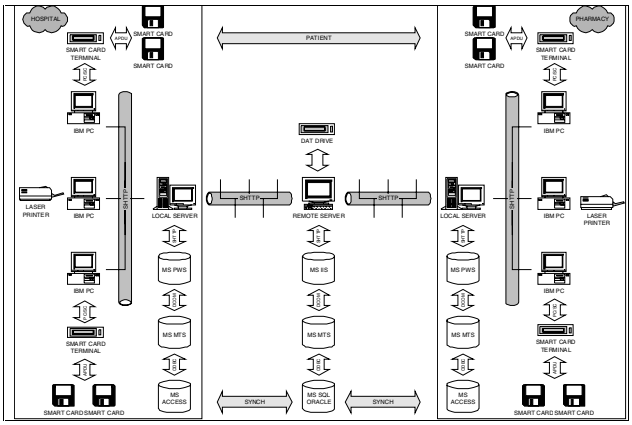

Figure 1: The proposed system's design in order to implement the government project for the separation of the dispensary from the doctors office in the Republic of Korea. The proposed system presents a secure transmission of a patient's medical prescription from the hospital to the pharmacy via the Internet/Intranet and the concurrently parallel co-operation with both patient's and professional's smart cards in the 2-way double-type terminal under the synchronized status.

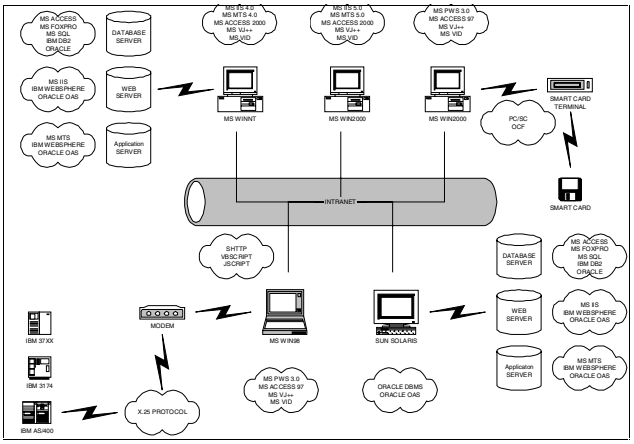

Figure 2: The secure Internet/Intranet and smart card terminals consist of all computer machines in a healthcare center over the secure HTTP or SSL protocols based on TCP/IP.

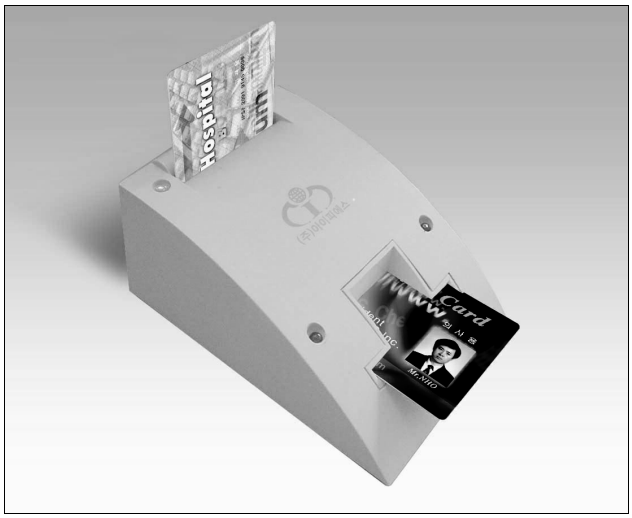

Figure 3: The 2-way double-type smartcard terminal which has two smartcard readers for a patient at left and for a medical professional at right within one body, respectively. That 2-way terminal is produced by IPS incorporation, Daejeon, Republic of Korea.

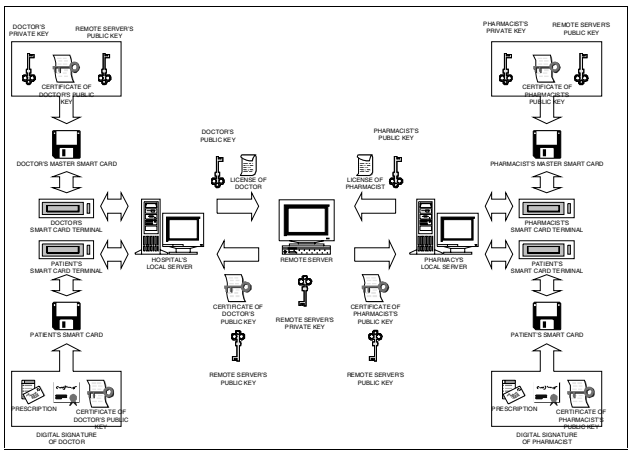

Figure 4: The digital signature and certificate have been issued under the public-key infrastructure environment. Each medical professional's smart card includes the own private and public keys, the digital certificate for own public key, and the public key of the remote server. Each patient's smart card has prescriptions, digital signatures for each prescription, and the digital certificate of medical professional's public key. The remote server at center plays a role of publishing the digital certificate of a medical professional's public key after an administrator checks the paper licenses of the medical doctors and pharmacists.