Electronic Healthcare Model Based on Smart Card For Saudi Medical Centers

Ebtisam Alabdulqader[1], **and H. Fourar-Laidi**[2]
[1] Information Technology Department / [2] Information Systems Department,
College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia

Abstract - *This paper presents a healthcare model based on smart cards. The purpose of the proposed model is to facilitate information exchange and integration across medical organizations. Currently, in Saudi Arabia, all medical centers have their own healthcare system. Each time a patient visits a clinic; a new file is created for him. Clinical information history related to the previous consultations is not available. Confidential information is not protected by the traditional folder. Prescriptions provided by doctors are signed manually and not efficiently authenticated by pharmacies. Claims are transmitted to the insurance companies by fax which makes them subject to falsification. The existing approach of the ministry of health in maintaining information about patients is not efficient, because healthcare institutions are not linked to a central system. In the proposed solution, the smart card will be used to store medical history of a patient that contains all diagnosis and drug prescriptions done in different medical centers. It will be used also to store keys and perform all the cryptographic computations. The medical institutions should adhere to the government healthcare organization system managed by the ministry of health. The healthcare organization should play the trusted third party as certification authority (CA). The information exchanged by the medical institutions should be protected and secured.*

Keywords: Healthcare, Smart card, Cryptography, Medical record, PKI

1 Introduction

Smart cards have been used by many countries to deploy healthcare programs [1, 2]. The smart card issued by healthcare organizations can be read easily with an appropriate smart card reading device and facilitates the secure sharing of patient clinical data amongst multiple healthcare providers. Smart cards can be used by healthcare institutions to considerably reduce the administrative work. Patients will no longer be requested to fill their personal information and describe their medical history each time they visit a healthcare institution. The proposed solution aims to use the smart card as portable storage device for clinical information that can be shared between healthcare institutions. Our approach consist on a integrated solution that use the smart card to perform secure transactions between the medical center, the insurance company, the pharmacy and the trusted healthcare organization.

In the proposed approach, each time a patient visits a medical center, he presents his health card. The medical center will use the card to authenticate the patient and retrieve all needed information and clinical records history. The clinic can also update the card by information related to the current visit. The health card is protected by a Personal Identification Number (PIN) known only by the patient. Retrieving confidential information and updating the card is performed by presenting the card PIN. The information stored in the card is synchronized with a central healthcare system to assure coherence and availability of information in case of lost, or in case the patient visits another medical center. The central healthcare system should be managed by a government organization like the ministry of health. The prescriptions given by doctors are electronically signed and sent to the pharmacy central service, part of the central healthcare system. Doctors cannot deny their prescriptions. Pharmacies can claim their money directly from the insurance company after authorization given by the patient. The pharmacy submits a request to the insurance company. Once the transaction approved, a response is sent to the pharmacy for completion. The transaction between the pharmacy and the insurance company is performed securely by using keys and certificates stored in the smart card.

Due to their cryptographic capability and portability, Smart cards are an ideal secure storage device that can be used to store and secure patient records. Smart card will be used also to secure the information exchange between the clinic access point and the central healthcare system using digital signatures, certificates and keys. The proposed model will be implemented and distributed among the medical centers (clients). In our project, we did not implement the transaction service between the pharmacy and the insurance company. The developed prototype includes the transactions between the patient, medical center and the healthcare central system. The use of smart cards to secure transactions assures more protection for sensitive data. Smart cards reduce the threat of unauthorized access by the use of stolen credentials because the hacker must both steal the smart card and obtain the PIN. The proposed model also offers more flexibility to the current

healthcare system by allowing patients to have rapid access to their electronic medical folder in any medical center. Patients do not need any more to redo medical tests each time they are changing clinic. This paper is structured as follows: in section 2, we present some healthcare models based on smart cards. Section 3 describes our proposed smart card healthcare model and its architecture. In section 4, we illustrate the implementation of the healthcare model using MULTOS technology.

2 Healthcare Models

Smart cards offer a new perspective for healthcare applications due to the security level provided for data storage. Smart cards in healthcare applications can be used for storing information including personal data, insurance policy, emergency medical information, hospital admission data and recent medical records [3]. Numerous healthcare systems around the world start using smart cards to improve the quality of healthcare services [4]. Different healthcare models have been proposed either on national level; e.g. in Germany [5] or regional level; e.g. in US. [6].

One of the interesting orientations ongoing is the attempt to further standardize and develop a framework to support Web-based medical-specific smart card applications [7, 9]. Many countries started developing healthcare programs based on smart cards. Here are three health-related examples. In Germany, the Krankenversichertenkarte is used to manage billing to various health-insurance companies for all services received by the public. Ontario plans to use a smart card to reduce fraudulent access to public health services.

"Carte Vitale" is one of the healthcare models issued in France with the aim to automate the paperwork flow between doctors, patients and insurance companies. Another healthcare model was an extending to the national ID card in Malaysia by adding health information as a function on this card which can only be read by medical professional. This health information provides next of kin contact details, detailed information on lifetime health history, hospital admissions and recent treatments [8]. The goal is to streamline treatment, reduce test duplication and automate interactions between patients, healthcare providers and payer organizations.

Chan et al. propose a vertical standard framework that addresses the design requirements specific to the development of medical applications [9]. The concept of the Java Card Web Servlet (JCWS) was developed to provide a seamless access interface between a Web browser and a Java Card-enabled smart card. In essence, the smart card is viewed as a repository of Web-enabled objects comprised of applets, HTML page, data objects, and Java Card applets. The framework supports tight integration of smart card technology with an existing Web infrastructure. Therefore, a hospital with a Java-compliant smart card reader is able to access medical information directly from the card using a standard Web browser via the JCWS. An applet contained within the card can be dynamically loaded into the browser to browse and update medical information. The applet can also provide Web links to Internet databases to facilitate wide area access of further information such as a video of a recent CT scan, high-resolution X-ray image scans, and so forth. The JCWS binds the database to the framework, while providing Web-based browsing and updating services. In this case, the browsing and updating applet can be downloaded from the smart card itself via the browser interface.

Another model was proposed by Song and co. this involved transferring medical prescriptions from the medical center to the pharmacy via the internet based on 2-way double-type smart card terminal. This later is used to control security and privacy of patients and manage drug histories of them [10]. 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. Finally, Attiaoui and al. describe an approach of using the Web USB smart card service model as a common interface to communicate and access the medical records residing in a smart card that seamlessly integrate to existing Web infrastructure [11].

3 The Smart Card Healthcare Model

Healthcare sector in Saudi Arabia needs simple identity cards for all patients to grant access to certain data in anywhere and at anytime. The proposed smart card healthcare model represents an alternative solution to improve the whole healthcare infrastructure by adopting a comprehensive multifunctional smart card system. The essential idea is based on multifunction smart card that is used as identity for patient authentication and stores medical data along with secure interchange of these data which will be used in various locations, such as hospitals, clinics and ambulances. According to that, the model will support both availability and security of the medical data.

A health smart card will be issued for each patient to replace their paper based medical record that is currently used in the region. The smart card will be utilized to store only the critical medical record information needed for each clinic visit and emergency cases. This limitation is due to the limited capacity of the currently available smart cards. The critical medical record information that will be stored on the smart card includes the personal and emergency contact information, urgent medical data such as allergies and list of current medications if any, as well as the latest patient medical examinations and prescriptions.

3.1 Architecture of the proposed model

The smart card healthcare model consists of three components that consist of the patient's smart card, the client

terminals and the central system located in the ministry of health as shown in Figure.1.

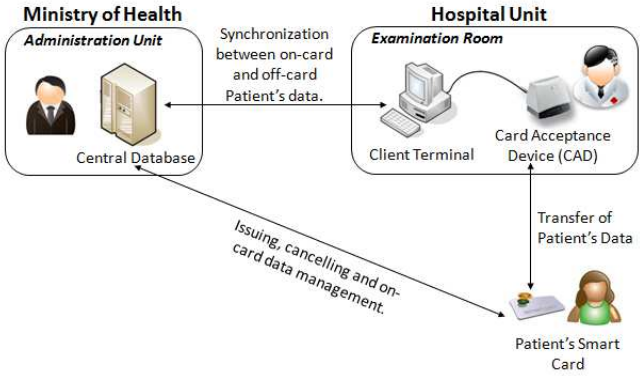

Fig.1 - Smart Card Healthcare Model Architecture.

The model introduces a hybrid solution in which patient's smart card is used in the system depending on the availability of the network. The patient's smart card will be used as a medical data carrier which can be accessed without any need for network connection to access the central system. It is also used to access additional patient medical data stored in the central system located in the ministry of health if the network connection is available.

In the first option, the data stored in the patient smart card (on-card) can be accessed quickly by the healthcare professional through the client terminal without any need for network connection to access the central system. This data include the latest medical record of the patient with medical examinations and prescriptions, personal information, emergency contact information, allergies and current medications. By this way, the model supports the medical data portability even with off-line client terminals when there is no connection to the central system.

On the other hand, patient's smart card can be used by the healthcare professional through the client terminal to access the healthcare organization system in case the network is available. This allows the healthcare professional to reach the remaining patient medical data stored in the central system and make an update with the information related to the current visit. The central system will store the additional medical data of the patient which is already stored in the medical card. By including a copy of the patient's card data in the central system, the healthcare organization will be able to recover the patient medical data and re-issue another card in case of lost or damage of the patient's smart card.

The second component of the system is the client terminal located in several locations in the medical centers. These terminals will be used by healthcare professionals to access the medical data stored on the patient card using the smart card reader which is connected or embedded to each client terminal [12]. A secure channel is established between the client terminal and the patient smart inserted into the reader. The transmission of patient's medical data will take place between patient card and client terminal.

In on-line communication, the client terminal is connected to the central system and exchanging patient information. The central system use to synchronize via the client terminal with the patient medical card by addition new information related to the last examination and prescription done by the healthcare professional. While if the client terminal is off-line, the synchronization will be done in the next connection of the patient smart card. Each time the client terminal is connected to the central system, a synchronization process is started by the central system. The synchronization process will synchronize the central system with the patient medical card and record the new medical examination and the related prescription stored on smart medical card. Consequently this will insure the availability of the latest medical data in case of lost or damage of the patient medical card.

3.2 Patient smart card communication session

The software running on the client terminal allows the healthcare professional to communicate with the patient smart card and carry out the examination. The communication between the client terminal and the patient's smart card is shown in Figure.2.

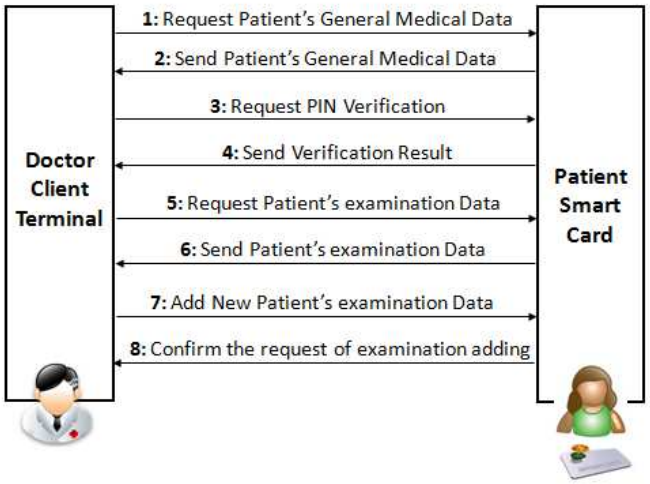

Fig.2 - Patient Smart Card Communication Session.

In general, communication can only be opened by a patient smart card. When a patient smart card is inserted in the reader, the healthcare professional can access the personal and emergency information of the patient directly without any verification. In order to access the latest examinations and prescriptions as well as the confidential information, the PIN is requested from the card owner. If the PIN is valid, the client terminal communicates with the patient smart card in

order to exchange the latest examination information. The information exchange between the client terminal and the card concerns retrieving information from the card and updating the card with information related to the current visit. Once the examination done, healthcare professionals can add new medical information and prescription on the patient smart card.

In every step of patient smart card communication session, the patient should be located in the same location of the smart card reader. In addition, if any changes have been made during the session or the visit, and the client terminal is in on-line state with the central system, a synchronization request will be automatically issued through the client terminal and sent to the central system. The purpose of this request is to synchronize the central system with the new patient medical card by adding information related to the current visit. In this case, the complete patient medical data will be available in the central system and the two sides (patient medical card and central system) are synchronized. Otherwise, if the client terminal is in off-line state, the changes will be marked to be synchronized in the next session when the connection between the client terminal and the central system will be available. This design will allow the healthcare organization the possibility to make another copy of the patient medical card if this later is lost or damaged.

3.3 The clinic healthcare service (Client)

The clinic healthcare services provided through client terminals will communicate with the patient smart card through the connected smart card reader. This service allows the healthcare professional to carry out examinations and record all related data. Through any client terminal, the healthcare professional can directly access the client personal information, emergency contact, allergies and current medications if any. This service is useful in urgent situation, such as, when the patient is unconscious state.

Moreover, after verification process, which is one of the services as well, the healthcare professional can navigate through the latest medical record of the patient with medical examinations and corresponding prescription and add a new medical examinations and its related prescription information on patient smart card if needed. An additional service should be implemented in the on-line terminal is the synchronization service. The synchronization service synchronizes the patient medical data stored in the smart card to the central system with the new patient medical data already stored in the card.

A ministry unit is responsible for carrying out the system administration functions through their terminals. Mainly, that unit is responsible to manage the central system which holds patients medical records. This unit is also responsible to record the patient's information into the system and to perform the related operations like issuing and cancelling smart card for patients. A synchronization service is integrated in the system that will allow having two data supports close to each other. Due their capacity limitation, we are storing examination information related to only the ten last visits. To be able to see the other visit information, the client terminal should be on line mode with the central system in order to retrieve needed information not available in the patient card. The ministry healthcare organization can recover the patient medical data and re-issue a new patient smart card in case of loss or damage.

3.4 The ministry healthcare service

A ministry unit is responsible for carrying out the system administration functions through their terminals. Mainly, that unit is responsible to manage the central system which holds patients medical records. This unit is also responsible to record the patient's information into the system and to perform the related operations like issuing and cancelling smart card for patients. A synchronization service is integrated in the system that will allow having two data supports close to each other. Due their capacity limitation, we are storing examination information related to only the ten last visits. To be able to see the other visit information, the client terminal should be on line mode with the central system in order to retrieve needed information not available in the patient card. The ministry healthcare organization can recover the patient medical data and re-issue a new patient smart card in case of loss or damage.

4 Implementation of an Electronic Healthcare System

The proposed smart card healthcare model has been implemented to validate our approach [13]. Our motivation in using this technology is the capability of the smart card to store, protect and manipulate medical data in a secure way. MULTOS Application Developer Smart Card has been chosen to implement the patient's smart card. MULTOS is an open multi-applications operating system that is ideal for the security need of our application [14, 15]. The advantage of this system is that many applications can run on the same card. The MULTOS card was used as patient's smart card to store the required amount of patient medical data.

The two applications developed are the application loaded into the smart card and the doctor's client terminal application. The data communication between the patient's card and the doctor's client terminal can start once the card is inserted into the reader. This will allow the doctor's client terminal to have access to the patient medical data and to update the card with the information related to the current visit. The patient's smart card application is responsible to handle the stored medical data on the smart card, while the doctor's client terminal application is an interface connected with a smart card reader. The information exchange between the doctor's client terminal and the central system will be done in a secure way using keys stored in the card. Confidential information is transmitted to the central system using an RSA algorithm. The content of the message is

encrypted by the RSA function using the public key of the healthcare organization stored in the card. The same message is decrypted using the RSA function using the healthcare organization private key. Some confidential information is not accessible only if the patient enters the PIN card. Also, updating the medical card with data related to the current visit by the doctor's client terminal is done with the authorization of the patient by entering the PIN. The client terminal application will interact with the smart card application by sending and receiving APDU (Application Protocol Data Unit) to exchange the medical data between the client terminal and the smart card in a secure way.

The patient's smart card application has a hierarchical modular structure. It consists of three levels, where each level is responsible to handle specific part of the data, as shown in Figure.3. The *HealthAPDU* module is the first level of abstraction. It defines the external interface with the smart card. It is responsible to handle all communications involving APDU operations that can be executed by the card. The *HealthATL* module introduces a second level of abstraction that can communicates with the low level module (*HealthAPDU*) and the high level module (*SCHS GUI*). The *HealthATL* module implements functions like *OpenSession* that call the *HealthAPDU* commands: *allocOpenCard, establishContext, connectToCard* and *selectFileByAid.* These APDU commands allocate the card structure, establishes the resource manager context with the card if no session is opened with the card, connect to the card if the smart card is inserted in the reader, and select the healthcare application. If the command is not executed as expected, these functions should return a specific error code. This error code is interpreted by the *HealthATL* module and a specific error message is displayed.

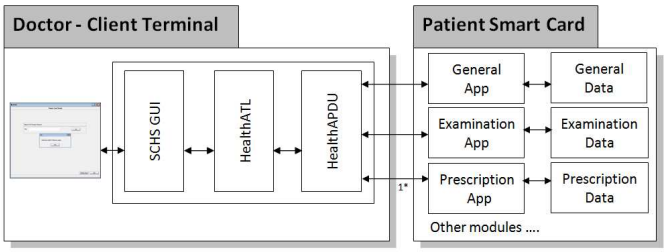

Fig.3 - Architecture of the Smart Card Healthcare System.

Patient's smart card application has three modules. Each module stores and processes a group of medical data. These modules can be accessed by client terminal to exchange the medical data. Each smart card module has a buffer for more than 200 characters to store a group of a related medical data into the smart card and defines a specific instruction to process these data. For example, Prescription Application which when loaded into the smart card is responsible for all patients' prescription data. These applications contains the related functions such retrieving and sending these data to the client terminal application or writing a new prescription on the patient's smart card.

The client terminal communicates and exchanges medical data with the patient's smart card module. It is implemented through three levels. Each level groups the related commands to allow communication with the smart card reader. Running commands is performed by sending APDU buffer to the smart card. These APDU commands read the responses sent from the smart card that specifies the execution status. In case of failure, the patient's smart card should return an error code. These three levels have been depicted in Figure.3.

The real communication with the smart card is performed in the lowest level of the client terminal. The communication with the card include connecting to the card, selecting the related application, sending APDU command to read or write medical data in the related module, and finally disconnecting from the card. The middle level module of the client terminal (*HealthATL*) interacts with both the lowest and highest level. The *HealthATL* module is responsible for preparing and manipulating patient's data before sending them to the next level (HealthAPDU). The highest level of client terminal application (*SCHS GUI*) handles the graphical user interface operations. The SCHS GUI takes the entered patient's data related to the current visit and sends them to the *HealthATL* module to be prepared for the *HealthAPDU* module. The *HealthAPDU* module sends the command through an APDU buffer to the smart card and the received response or the error code to the *HealthATL*. Once received, the *SCHS GUI* displays the patient's data requested, or a message that confirm the update, or a message error explaining the problem.

The client terminal system has a modular structure and has been designed within three levels. Each level contains one specific module. The patient's smart card application also has been divided over several modules and data groups as show in the figure.3. This architecture will facilitate modification, because each group of the medical data is stored in a separate module. The change will affect only in one module. Also, if we need to implement another application for the healthcare professionals for example, we can use modules like *HealthAPDU* to communicate with the smart card. Some of the client terminal applications will interact only with a specific group of the medical data and prevented from the interaction with other data. Thus, this modular structure offers data protection and ensures that the client terminal application interacts with the required module only. The pharmacy client application will interact with prescription smart card module only. An administrative personalization tool was developed to load experimental data, keys and certificates.

5 Conclusion

The smart card healthcare model was developed to allow each patient to carry a secure medical record in a smart card and use it in the authentication processes and emergency

cases. This model aims to improve the quality of smart card services in the healthcare sector in the region. Additionally, the smart card services in healthcare sector will be enhanced with the increase capacity and lower costs of the smart cards with a higher capacity. Smart card would have the capability of storing extra medical information such as x-ray images.

The smart card healthcare model can be extended to integrate healthcare professional's data. These cards will store the healthcare professional personal information needed by the medical centers. Consequently, each healthcare professional can be authenticated using their own card and will able to access the patient's medical data with the patient's card. In the proposed model, the healthcare professionals can retrieve data and update the smart card only if the patient enters his PIN. In the next step, the healthcare professional will not be allowed to update the card or to execute any transaction if he doesn't insert his card first and enter his PIN. In this case, each transaction data present in the smart card is allowed and identified.

Furthermore, pharmacies and insurance companies can be integrated in the model to process the electronic prescriptions currently stored in smart cards. The pharmacies can proceed the prescriptions only when they receive an approval from the insurance companies. Hence, that will provide a paperless communication between hospitals, pharmacies and insurance companies.

The insurances companies should adhere to the ministry health organization in order to trust the reimbursement request coming from the pharmacies. The healthcare organization will play the trust party of the pharmacy and the insurance company. The healthcare organization will permit the reimbursement transaction. Due to the modular architecture, those modifications can be added in the proposed healthcare model. The government healthcare organization can also revoke the certificate for a healthcare professional. This alternative was not included in the developed prototype. In this case, the healthcare organization will reject the transaction request made by the healthcare professionals.

6 References

[1] Kardas G. and Tunali E. T. "Design and implementation of a smart card based healthcare information system". Computer Methods Programs Biomedicine, 81, 1 66-78, Jan. 2006.

[2] Moon D., Chung Y., Pan S. B., and Park J. "Integrating fingerprint verification into the smart card-based healthcare information system". EURASIP J. Adv. Signal Process, 5-5, Jan. 2009. DOI= http://dx.doi.org/10.1155/2009/845893

[3] Mayes K., Markantonakis K.. "Smart Cards, Tokens, Security and Applications", Springer, 2008.

[4] A. Alkhateeb, T. Takahashi, S. Mandil, and Y. Sekita. "The changing role of health care IC card systems". Computer Methods & Programs in Biomedicine, 60, 2, 83-92, 1999.

[5] M. Marschollek and E. Demirbilek. "Providing longitudinal health care information with the new German Health Card - a pilot system to track patient pathways". Computer Methods & Programs in Biomedicine, 81, 3, 266-271, 2006.

[6] Savostyanova N. and Velichko V. "Plastic card fraud: a survey of current relevant card and system properties", 2004.

[7] Bernd Blodel and Peter Pharow. "A model driven approach for the German health telematics architectural framework and security infrastructure". International Journal of Medical Informatics, 76, 169-175, 2007.

[8] Rankl W. and Effing W. "Smart card handbook", Wiley & Sons, 2003.

[9] Alvin T.S. Chan, Jiannong Cao, Henry Chan, and Gilbert Young. "A Web-Enabled FRAMEWORK for SMART CARD Application in Health Services". COMMUNICATIONS OF THE ACM, 44, 9, 77-82, September 2001.

[10] Won Jay SONG, Byung Ha AHN and Won Hee KIM. "Healthcare Information Systems Using Digital Signature and Synchronized Smart Cards via the Internet". Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'02) IEEE Computer Society.

[11] Walid ATTIAOUI, Pr. Mohamed BEN AHMED, Pr. Moncef TAGINA and Dr. Boutheina CHETALI. "Integrating USB Smart Card with Flash Memory to Web based Medical Information Systems: Application for the pathology of cancer", IEEE Explore, 971-977, 2006.

[12] Rodrigues R., Piccolo U., Hernandez A. and Oliveri N. "Integrated circuit Health data Cards", Pan American Health Organization, 2003.

[13] Ebtisam AlAbdulqader. "Smart Card in Healthcare Systems". Project Report submitted for the degree of Master in Information Systems, College of Computer and Information Sciences, King Saud University, June 2009.

[14] "Multos development tools and manuals". Available at: http://www.multos.com/

[15] Hendry M." Multi-application Smart Cards: Technology and Applications". Cambridge University, 2007.