Experience developing a healthcare smartcard system

Surgeons working in operating rooms today need to access a growing mass of information. How should hospitals manage and display data, so that it is both handy and flexible?

Geylani Kardas PhD

Ege University
International Computer Institute
Izmir, Turkey

Have **your** say!

Email us at:
hite-feedback@campden.com

For the smart view, click online ...
hospitaliteurope.com

Smart cards are plastic cards resembling traditional credit or debit cards with embedded integrated circuits that can both store and process data. Most of the advanced types of these cards include a data-processing unit (or CPU – central processing unit) and various types of memory – ROM (read-only memory), RAM (random access memory) and EEPROM (electrical erasable programmable read-only memory) – for data storage. Hence, in fact, these cards can be viewed as tiny portable computers.

Smart cards are used in various business domains (eg, banking systems, telecommunications and transportation) to provide a flexible, secure and standard method for business transactions with minimal human intervention. The use of smart cards in healthcare information systems also became very popular since smart cards appear to be the most suitable media to be used when we consider the strong requirements of these systems regarding identification, authentication, security and data storage.

Recently, we developed a smartcard-based healthcare system (SCHS) with the collaboration of healthcare professionals employed in the Neurosurgery Department of Ege University Hospital. The developed system includes smartcard usage in data flow and provides data communication via a distributed protocol. Smart cards are used both for mobile data transmission and security and authentication purposes in the system.

In the following, the system and the experience gained during its development are summarised. Detailed information on the design and implementation of the SCHS can be found in Kardas and Tunali (2006).[1]

The implemented system

In SCHS, both patients and doctors have smart cards. Doctors use their cards to be authenticated in the system, while patient cards include the owner's general health information, which can be accessed without any database connection. There exists a central hospital to store on-card and off-card health data. Department/clinic-specific patient data are stored on local databases of related departments, and the system also interacts with them over a distributed protocol. Therefore, the system provides availability of limited but important health information at presence of the card, as well as database access if possible.

Security of patient information and authentication of the doctors are vital for the system. A secure channel is established between terminals in examination rooms and card acceptance devices (CADs) connected to those terminals. When a doctor or patient smart card is inserted in a CAD, authentication is assured between card and host computer software by key exchange. Then the card access PIN (personal identification number) is requested from the card owner, and the entered PIN is checked by the smart card itself. The smartcard session is then opened unless the entered PIN is wrong. Database access from client terminals is also realised via a secure distributed system protocol. Data are transmitted in an encrypted form over the protocol's channel. To provide authentication of doctors for the system and their access to system servers, private digital signatures stored on doctor smart cards are used.

Computers located in examination rooms are defined as system client terminals. Each terminal has a connected CAD, and they can connect to

specific system servers to access databases. The software running on terminals can open doctor and patient sessions. There must be an open doctor session to accept patients and carry out examinations.

An examination based on a smartcard session is realised as follows: When the patient card session is opened, the terminal receives requested data from the clinic server in an encrypted form. Data are encrypted with a patient key on the server side, and to decrypt on the client side the terminal needs the same key stored on the patient smart card. In addition to the general health information, decrypted clinic-specific patient health data are displayed. After examination, the doctor updates inspection and prescription information on the patient smart card with new data, and he/she also updates clinic-specific patient data if he/she has authority. Updated clinic-specific data are again encrypted using the patient encryption key, signed with the doctor's private digital signature and sent to the remote clinic server. The reverse procedure is carried out on the server side: the signature is verified with the doctor's public key, and patient data are decrypted again with the patient's key. Data updating on the clinic database is completed if everything is in order. The result of the remote process is returned to the terminal and the patient session is closed. Finally, the patient applies to the system administration unit to transfer new inspection and prescription data stored on the smart card to the hospital database and to enable prescription approval.

System development experience from the IT developer's perspective

Capturing the user requirements

Naturally, both healthcare professionals and patients expect a system in which patient acceptance and examination procedures are carried out accurately and quickly. An extensive investigation of clinical requirements in the Neurosurgery Department was made. Ongoing healthcare processes and health information systems in the hospital were examined in detail, and subsequent integration of requirements into the SCHS's functional specification was realised.

Such an examination of the current system was extremely important because doctors especially emphasised the need for a new smartcard-based system that would have the same execution procedures as the previous system but would work in a more secure and quicker way. They even requested the same graphical user interfaces, to which they got accustomed in the previous system.

The implemented system met all of these user requirements through its modular software architecture design.

Determination of the amount and type of data stored on smart cards

Keeping all health records on a smart card is impossible, and if it were possible it would cause system management problems in cases of lost or damaged user cards. On the other hand, use of smart cards only as a media to access health data already stored on a network was not appropriate for the desired SCHS capabilities. The chosen way was to determine the essential system information (eg, encryption keys, digital signatures and database connectivity parameters), calculate the data space needed on cards for that information and then keep the amount and variety of the health data at that maximum.

As the application developers, we also had to consider the memory and storage needs of on-card software applications. Those applications would be executed at the runtime of the smart cards in order to process the stored health data. Since smart cards have really very small (almost negligible) memory and storage sizes compared with personal computers, application developers always have to deal with that challenge during smartcard-based system design.

Of course, the type of health data on smart cards can vary according to the system requirements. For instance, in our system, we kept unique patient ID and card access PIN, patient personal information, emergency contact information (name, surname, home, work and mobile phone numbers of the person to be contacted and his/her relationship with patient) and insurance information inside the card. We grouped patient health information stored in the card as follows: chronic and/or important former diseases with diagnosis dates, permanently used medications with doses, allergies with diagnosis dates, immunisations with their dates, surgical operations including operation date, clinic name and summary information. The patient's last examination and prescription information were also stored on the card.

Another issue is the use of card security capabilities in an effective and appropriate manner. Keeping the entire data password protected and/or encrypted could cause system inadequacies. For instance, in our implementation, both patient personal information and emergency contact information in patient smart cards were not PIN protected. Especially in an emergency condition, it may not be possible to obtain the PIN from a patient. In such conditions, the card provides personal data and contact information without any PIN entry.

Cooperation with healthcare professionals

During requirement determination, domain analysis and evaluation phases of the SCHS, a collaborative study was performed with the healthcare professionals. Assessment of the system by the professionals is critical to determine the strengths and weaknesses.[2] Considering the SCHS evaluation, doctors in the Neurosurgery Department preferred a practical assessment based on their experience instead of a methodological one.

Adaptation of the users

Inevitably, we experienced some initial difficulty in deploying the new healthcare system in an environment in which some users were addicted to the legacy system. However, we did not meet with any particularly strong resistance against the new system, largely because users found a new application on their desktop with almost the same user interface as and similar working mechanism to the legacy system.

Conclusion

Design and implementation of smartcard-based healthcare systems is always challenging, especially considering the hardware/software boundaries. The very limited smartcard resources should be assigned carefully and used efficiently to provide maximum satisfaction for both healthcare professionals and patients.

However, based on a complete requirements analysis and an appropriate system design, such smartcard-based systems can provide security, authentication, rapidity and easy-to-use features for healthcare IT applications. ■

References

1. Kardas G, Tunali ET. Design and implementation of a smart card based healthcare information system. *Comput Methods Programs Biomed* 2006;81(1):66-78.
2. Heathfield H, Pitty D, Hanka R. Evaluating information technology in health care: barriers and challenges. *Br Med J* 1998;316(7149): 1959-61.