A Secure Framework and Related Protocols for Ubiquitous Access to Electronic Health Records Using Java SIM Cards

Reza Hassanzadeh, Tony Sahama, and Colin Fidge

Faculty of Science and Technology
Queensland University of Technology
Brisbane, Australia
r.hassanzadeh@isi.qut.edu.au,
{t.sahama,c.fidge}@qut.edu.au

Abstract. Ubiquitous access to patient medical records is an important aspect of caring for patient safety. Unavailability of sufficient medical information at the patient point-of-care could possibly lead to a fatality. In this paper we propose employing emergent technologies such as *Java SIM Cards* (JSC), *Smart Phones* (SP), *Next Generation Networks* (NGN), *Near Field Communications* (NFC), *Public Key Infrastructure* (PKI), and *Biometric Identification* to develop a secure framework and related protocols for ubiquitous access to *Electronic Health Records* (EHRs). A partial EHR contained within a JSC can be used at the patient point-of-care in order to help quick diagnosis of a patient's problems. The full EHR can be accessed from an Electronic Healthcare Records Centre (EHRC).

Keywords: Electronic Healthcare Record, Java SIM Card , Next Generation Network, Smart Phone, Near Field communication, Biometric Identification, Public Key Infrastructure.

1 Introduction

Ubiquitous access to a patient's medical records is an important aspect of caring for patient safety. Unavailability of sufficient medical information at the patient point-of-care could possibly lead to a fatality. The U.S. Institute of Medicine (IOM) has reported that between 44,000 to 98,000 people die each year due to medical errors, such as incorrect medication dosages due to poor legibility in manual records, or delays in consolidating needed medical information to discern the proper intervention. Also the IOM reports the lack of well designed systems and procedures needed to handle the complexity of health care distribution caused 90 percent of medical errors [1]. Most of these medical errors could be avoided with access to patient's medical information at the point of care [2]. Ubiquitous access to patient's medical information is a technique which enables Healthcare systems to have access to patient's medical information wherever it is needed electronically. It has the potential to revolutionize next generation medical applications based on *Electronic Health Records* (EHRs). It could significantly improve the quality of healthcare services to increase patient safety and reduce medical errors and costs.

H. Takeda (Ed.): E-Health 2010, IFIP AICT 335, pp. 102–113, 2010.

Therefore, in this paper, we propose a secure framework and related protocols by taking advantage of new technologies such as *Java SIM Cards* (JSC), *Smart Phones* (SP), *Next Generation Networks* (NGN), *Near Field Communications* (NFC), and *Biometric Identification* for ubiquitous access to patient's medical information at the point-of-care.

The aim of our framework and related protocols is to overcome pervious work's limitations by taking advantage of SIM cards and the new technologies mentioned above. Briefly, our approach could offer the full benefits of accessing an up-to-date, precise, and comprehensive medical history of a patient, whilst its mobility will provide access to medical and patient information everywhere it is needed.

2 Related Work

Ubiquitous Access to patient information has been investigated by many researchers such as Abraham [2], Issa [3], Chenhui [4], and others. Finding an efficient solution that can be secure and implemented in existing Medicare systems is a challenging issue. Some researchers such as Bishop [5] and Chan [6] have proposed using a Medicare card, which is based on a Smart Card, as a potential solution to access patient's health records anywhere and anytime.

However, using Medicare cards as a repository of medical information at the patient point-of-care imposes some limitations on patients' emergency medical care and privacy. These include the inability to detect and inform patient's location, call and send patient information to an emergency room automatically, and computerise and secure interaction with the patient. Our approach aims to overcome these limitations by exploiting the additional capabilities of *Java SIM Card* and new communication technologies.

3 Framework Overview

Our framework is based on developing a secure conceptual structure to enable an *Authorised Person* (AP) such as a doctor to have *Ubiquitous Access* (UA) to a patient's medical record on a national scale. As shown in Fig. 1, the proposed framework relies on new technologies such as *Java SIM Cards* (JSC), *Smart Phones* (SP), *Near Field Communications* (NFC), *Next Generation Networks* (NGN), *Public Key Infrastructure* (PKI), *Secure Sockets Layer/Transport Layer Security* (SSL/TLS) and *Biometric Identification* (BI).

This framework includes six major parts: the *Patient* (P), a *Smart Phone* (SP), an *Authorised Person* (AP), an *Authorised Device* (AD), a *Trusted Third Party* (TTP), and an *Electronic Health Record Centre* (EHRC). The TTP and the EHRC operate at the national (N-TTP, N-EHRC) and state (S-TTP, S-EHRC) levels. The SP is utilised to computerise interaction with a patient. The AD, which is a kind of a *Smart Phone* or *Personal Computer* (PC), is used by an AP such as a doctor to communicate with the SP or TTP. The N-EHRC is a central database containing all patients' EHRs on a national scale. The N-TTP is employed to manage the whole framework's activities. The S-TTP

and S-EHRC work at state levels. (For the purposes of this paper, we assume the existence of a central, national EHRC, as well as distributed state-level EHRCs; however the proposed communication framework does not rely crucially on having a centralised database. If necessary its functions can be distributed to the state level.)

Mobile phones, in general, fall into three broad categories: basic phones, multimedia phones, and *Smart Phones* [7]. A *Smart Phone* is a handheld device which has both mobile phone and PC-like abilities together. *Smart Phones* have become an emerging phenomenon for personal and business voice, data, e-mail, and Internet access, and could now form the basis of a healthcare network.

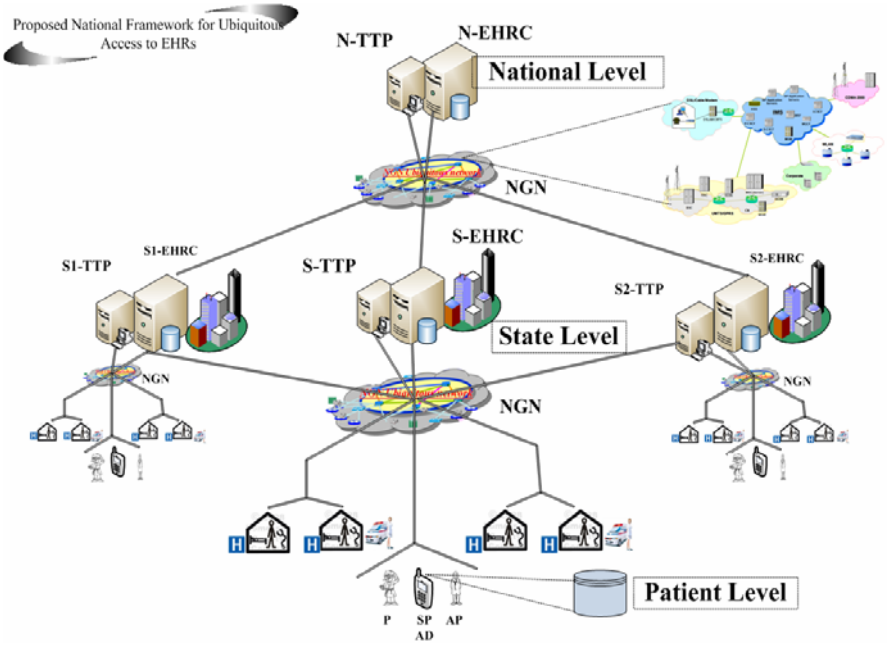

Fig. 1. National Framework for Managing Ubiquitous Electronic Health Records

The *Trusted Third Party* must be a powerful server which is able to manage very large amounts data and traffic. We assume it is facilitated with auditing, logging, authorisation, identification, and storage capabilities. Furthermore, the TTP must be connected to a database which contains all details of *Authorised Persons* and patients, including SIM IDs, devices' serial numbers, fingerprint templates, names and national IDs. Such a capability is now possible using current generation network servers from companies such as HP, IBM, or Dell.

The aforementioned characteristics of the SP, AD and TTP make them suitable for the needs of our framework. Our framework needs to provide ubiquitous access to a patient's EHR, have computerised interaction with a patient and AP, and have a central management system.

3.1 Proposed National Communication Framework

As shown in Fig. 1, our framework is divided into three levels: the national level, the state level, and the patient level. Each level has its own database which is responsible for storing patient medical records accordingly. Therefore, the framework includes three kinds of databases: a *National-Electronic Health Records Centre* (N-EHRC), *State-Electronic Health Records Centres* (S-EHRC), and patient databases (*Java SIM Cards*). Having both national and state databases is an effective strategy for achieving fault tolerance, better performance, and reliable access to large downloads of data.

The patient database stored in a JSC is responsible for storing critical medical information such as their past medical history, blood type, allergies, and the http links (*Uniform Resource Locator*) to the original records and medical images in the central database that we called the *Electronic Health Records Centre* (EHRC).

As the patient's point-of-care location cannot be prearranged, the *Java SIM Card*, due to its intrinsic nature of mobility, can play the role of a portable data repository to help quick diagnosis of a patient's problems. The JSC can make the patient's medical records available across the country or internationally even when the network is not available.

The *National-Electronic Health Record Centre* (N-EHRC) is a central database which contains all patients' EHRs on a national scale. It is responsible for storing the medical records for all the patients in a particular country. This database must be hosted and maintained by a government authorised organisation. The location of this database depends on the network topology in a particular country. The N prefix denotes the country's abbreviation, e.g., 'AU' for Australia and 'IR' for Iran. Therefore, the central database which contains all Australian medical records is designated the AU-EHRC.

The state database or *State-Electronic Health Record Centre* (S-EHRC) is the second tier database and is responsible for storing patients' EHRs at an intrastate level. The S-EHRC stores a copy of EHRs which belong to patients who reside in a specific state (or province or other relevant division within a country). This database must be hosted and maintained by a local government authority. Again the location of this database depends on the network topology in a particular country and state. The S-EHRC and N-EHRC work together to provide fault tolerance, better performance, and reliable access to EHRs. The S prefix denotes an abbreviation for the state within a country, e.g., 'QLD' for Queensland or 'NSW' for New South Wales. Hence, the central database which contains all Queensland's patients' medical records is designated the QLD-EHRC.

As shown in Fig. 1, the framework also includes two other entities the *National Trusted Third Party* (N-TTP) and the equivalent state-based *Trusted Third Parties* (S-TTP). The N-TTP operates on a national scale and S-TTPs work on an intrastate scale. The S-TTP is in charge of managing the *Smart Phones* and *Authorised Devices* while the N-TTP is responsible for managing the S-TTPs including authorising, updating, monitoring, enabling, and disabling the S-TTPs.

In terms of management, each S-TTP is responsible for managing all duties associated with the operation, communication, and maintenance of the SP, AD and S-EHRC within the particular state. For instance, the S-TTP determines an *Access Level* (AL) for the EHRs based on three factors: the identification of an *Authorised*

Device and *Authorised Person* who wants to have access to a patient's medical information, the patient's consent, and the relevant healthcare legislation. Based on these factors the S-TTP maintains three access control lists: *Discretionary Access Control* (DAC), *Mandatory Access Control* (MAC), and *Role Based Access Control* (RBAC) [8, 9]. The MAC and DAC list are made by using the patient's consent. The RBAC list is defined by legislators. The goal is to provide doctors, hospitals, and ambulances with a reasonable level of access to a patient's medical information while still preserving patient privacy.

Moreover, interoperability between different medical information systems which cannot communicate with each other is another of the S-TTP's responsibilities. They must be able to recognise a message's context and convert heterogeneous medical information into a unified format [4]. This allows medical information to be exchanged across different healthcare systems.

Accountability is possible only when the S-TTPs are able to provide strong security mechanisms such as access control, audit trails, and authentication of the patient, *Smart Phones, Authorised Persons*, and *Authorised Devices*. For example all access to the medical records must be logged and entered in an audit trail by the S-TTPs.

3.2 Data Security in the Framework

In terms of security, this framework relies on PKI, SSL/TLS, and *Biometric Identification*. The SSL/TLS protocol is used for implementing secure sessions between a *Smart Phone*, an *Authorised Device*, and a *Trusted Third Party*. The PKI is used by the SP and AD to generate *Non-Repudiable* messages. *Biometric Identification* is employed to ensure that only *Authorised Persons* can access a patient's medical information. PKI is an IT infrastructure which includes a set of procedures, policies, software, hardware, and network services that support security mechanisms such as confidentiality, integrity, authentication, and non-repudiation [10]. PKI utilises public and private keys for encryption and decryption of sensitive information [11].

Biometrics refers to automated techniques for uniquely recognising a person based on a natural physiological or behavioural feature. Features such as the face, fingerprints, hand geometry, handwriting, iris patterns, retinal patterns, veins, and voice are measured for recognition. Biometric technologies are emerging as a foundation of extremely secure identification and personal verification solutions [12].

3.3 Wireless Communications in the Framework

In relation to IP-Wireless and contactless communication, the framework uses *Next Generation Network* and *Near Field Communication* technologies respectively. The NGN is utilised to establish *Internet Protocol* (IP) based wireless communication between the *Smart Phone* and *Trusted Third Party*, and the *Authorised Device* and TTP. The NFC is used to facilitate contactless communication between the AD and SP.

A *Next Generation Network* is an IP-based network that handles multiple types of traffic (such as voice, data, and multimedia). It is the convergence of service provider networks including the *Public Switched Telephone Network* (PSTN), the Internet, and the wireless network [13]. We contend that it is possible to access a wide range

of ubiquitous e-health services through this unified network. *Java SIM Cards* are already used in the NGN for authentication, communication and security; we believe it is possible to expand those functionalities by using the JSC as a portable repository of EHR data at the patient point-of-care.

Near Field Communication is a wireless connectivity technology evolving from a combination of contactless identification and networking technologies [14]. It enables convenient short-range communication between electronic devices and smart objects. In our framework NFC plays the role of a contactless communication protocol between a *Smart Phone* and an *Authorised Device*. Through this technology patients can send their consent to the *Authorised Device* and an *Authorised Person* can see the patient's critical health information contained within a patient's device when it is needed. The communication protocols in which these devices can work together via NFC are outlined in Section 4.

3.4 Data Storage in the Framework

In terms of storing medical data our framework use two large databases at the national and state level and a portable small one which is carried by patients in their *Java SIM Cards*. This portable database is responsible for storing critical medical information.

A *Java SIM Card* is a *Subscriber Identity Module* (SIM) card for mobile networks which is made based on a *Java Card*. It is highly secure, efficient, easy to manage and provides many possibilities for supporting various applications [15], and is thus well-suited to storing healthcare records.

3.5 Proposed Local Communication Framework

As shown in Fig. 2, for the purpose of storing an individual's lifetime health information, the local framework contains two central databases called the *Australian-Electronic Health Record Centre* (AU-EHRC) and *Queensland-Electronic Health Record Centre* (QLD-EHRC) in our particular example. In addition, *Java SIM Cards* are used as a patient point-of-care medical information repository. The state level QLD-EHRC database includes only a copy of records for those patients who already live in Queensland or who temporarily visit the state. If a patient visits or moves to any state in Australia, other than his/her own state and needs medical care, the medical record is automatically fetched from the national database (AU-EHRC) and inserted into the visited state's database such as the QLD-EHRC. This strategy minimises traffic to the national AU-EHRC in a way similar to GSM mobile networks [16].

For the purpose of security, various mechanisms and protocols such as *Biometric Identification*, the *Secure Sockets Layer/Transport Layer Security* (SSL/TLS) protocol and *Public Key Infrastructure* encryption must be utilised to achieve secure access to patients' medical information. As we assume the communication between the *Smart Phone* or *Authorised Device* and S-TTP is based on a *Next Generation Network* which uses the Internet as a carrier, our framework must use PKI and SSL/TLS for the purpose of data confidentiality, integrity, authentication, and non-repudiation. These technologies enable the SP, AD, and TTP to exchange sensitive information through the unsecure public network. The patient's *Private Key* is stored in the *Java SIM Card*

which has the capability of operating cryptographic algorithms, while the patient's *Public Key* is stored by the AU-TTP and QLD-TTP.

Biometric Identification such as fingerprints must be used for accurately authenticating a patient or an AP. In principle, biometrics cannot be forgotten or lost, and are difficult to duplicate or share among different users [17]. A biometrics authentication system requires the physical presence of the individual. Among several biometric technologies, fingerprints have been in use for the longest time and have more advantages than others. For instance, there are many devices such as *Smart Phones* on the market that are equipped with a fingerprint scanner. A fingerprint is captured via live scan and then its features are retrieved. The retrieved fingerprint's features are then fed into the JSC, where the fingerprint template is stored, for the matching process. If a match is made, access to the medical information will be granted.

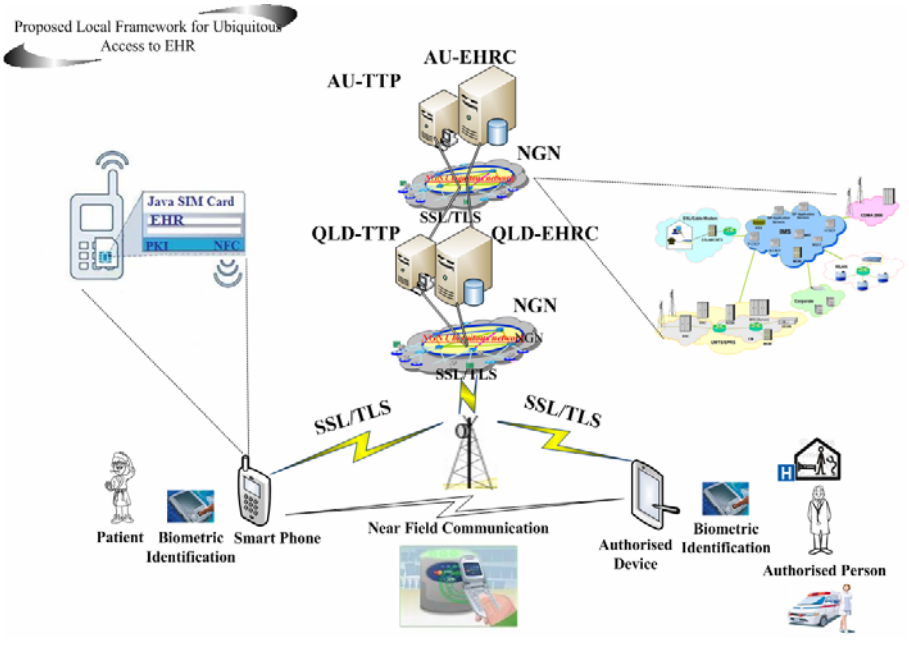

Fig. 2. Local Framework for Managing Ubiquitous Electronic Health Records

3.6 Contents of a Java SIM Card (JSC)

Fig. 3 splits the patient's *Java SIM Card* into three layers for managing ubiquitous Electronic Health Records: the application and database layer (*Applet Layer*), the *Java Card Runtime Environment* (JCRE) layer, and the *OS/Hardware* layer. While the JCRE and OS/HW layers are specific to a particular computing platform, we require an Applet Layer to address the design requirements specific to the development of *Ubiquitous Access to Electronic Health Records*.

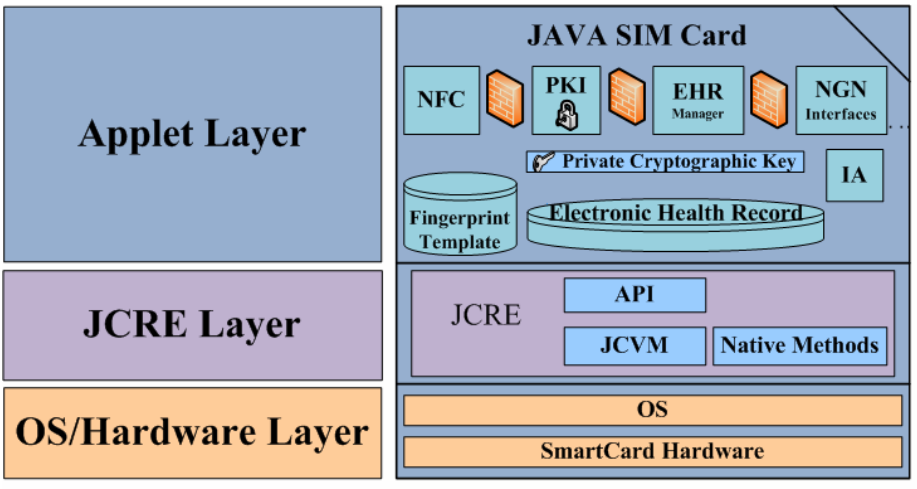

Fig. 3. Java SIM Card Architecture for Managing EHRs

The *Applet Layer* must consist of an EHR-Manager, PKI, NFC, *Identification Algorithm* (IA), NGN Interfaces and other applets as necessary. Additionally, this layer includes the *Private Cryptographic Key* and a small database which contains critical medical information such as past medical history, blood type, allergies, and the http links (Uniform Resource Locator) to original records and medical images in the central database.

The EHR-Manager interface is needed to handle communication between the state-level QLD-TTP and the *Java SIM Card* in order to update the EHRs contained within the *Java SIM Card*. After an *Authorised Person* updates a patient's EHRs within the QLD-EHRC, the QLD-TTP automatically updates the EHR within the JSC by using the *EHR-Manager* interface, *Smart Phone*, *Next Generation Network*, SSL/TLS protocol and *Over The Air* (OTA) and *SIM Tool Kit* (STK) technologies. OTA and STK technologies are widely adopted in mobile communication systems to read and write the contents of *Java SIM Cards* [18]. After a patient confirms the acknowledgement SMS message coming from the QLD-TTP, the update will be done.

The JSC must be equipped with a *Near Field Communication Application Programming Interface* (NFC API) in order to exchange information with an *Authorised Device* over about a 10 centimetre distance. The NFC enables the *Smart Phone* and *Authorised Device* to have contactless communication. By using the NFC a *Smart Phone* is able to send a patient's consent to the *Authorised Device* or the *Authorised Person* is able to see the patient's EHR within the JSC. There are many mobile phones such as the Nokia 6216 and 5800 in the market that support a SIM-based NFC interface.

The *Identification Algorithm* (IA) is needed for the challenge-response mechanism occurring between the *Smart Phone* or *Authorized Device* and the QLD-TTP. Challenge-response is important in the process of identifying a remote source as either an individual or a device. This algorithm works similarly to GSM authentication [19]. IA uses the challenge and the unique embedded information

which is stored within a tamper-resistant *Java SIM Card* to generate a *Fresh ID*. The unique embedded information include the SIM ID, device serial No, scanned Fingerprint, name, and National ID.

As shown in Fig. 3, the *Java SIM Card* must also be facilitated with a *Public Key Infrastructure* API in order to implement secure sessions between the SP and AD and QLD-TTP and produce *Non-Repudiable* messages. We assume that all the *Public Keys* of the patients who reside in QLD are stored in the QLD-TTP and it is responsible for managing them. Therefore, if the AD needs to communicate with the SP, it must first connect to the QLD-TTP to get the patient's *Public Key*. Moreover, the AU-TTP must be able to put the patients' *Private Keys* on their *Java SIM Cards* remotely by using *Over The Air* (OTA) and *SIM Tool Kit* (STK) technologies.

For the sake of clarity, we suppose that when the SP needs to send any information to the AD or QLD-TTP, this information must be encrypted by the *Private Key* which is contained within the patient's JSC. An *Authorised Device* or QLD-TTP can decrypt the message received from a *Smart Phone* by using the patient's *Public Key*. If the AD needs to send any information to the SP, first it must get the patient's *Public Key* from the QLD-TTP, and then it must encrypt the information with the patient's *Public Key*. The SP can decrypt the message received from the AD or QLD-TTP by using its own *Private Key* within the JSC.

The *Java SIM Card* is a multi-application environment. Multiple applets from different vendors can coexist in a single card, and additional applets can be downloaded after card manufacture. An applet often stores highly sensitive information, such as EHRs, fingerprints, private cryptographic keys, and so on. Sharing such sensitive data among applets must be carefully limited [20]. Therefore, for further security the JSC must have a firewall between the applets in order to achieve isolation and restrict access to the data of one applet from another as shown in Fig. 3.

Furthermore, in the case of the *Java SIM Card* being lost or stolen, the JSC can protect the information within the card by requiring a fingerprint and PIN code to access the patient's medical information. Also after the QLD-TTT is aware of a card going missing, it can remotely disable the card and delete all personal information inside the card.

4 Communication Protocols

In Section 3, we introduced a framework in which an Authorised Person such as a doctor is able to have Ubiquitous Access to a patient's medical record on a national scale. We also saw what components the framework needs and how the components fit together in general terms. In this section we briefly summarised the three different protocols needed for communication between the *Smart Phone* (SP), *Authorised Device* (AD), and *Trusted Third Party* (TTP). All three protocols work on the application layer which means they are independent of the underlying protocol layers for end-to-end communication. The application layer is the 7th layer in the Open Source Interconnection (OSI) reference model [21] and is closest to the end user. The SP, AD, and TTP protocols define the processes and procedures that must be followed when these agents want to request data from, respond to and communicate with each other. The protocols are designed to cover different emergency and non emergency scenarios.

The *Smart Phone* (SP) protocol is used when a patient wants to request data from, respond to, or communicate with *Authorised Devices* (AD) or a *Trusted Third Party* (TTP). In total the SP protocol requires seven major processes and procedures: *Authenticating the Patient*, *Modifying an Access Control List*, *Viewing EHRs*, *Identifying the Patient*, *Granting Consent*, *Generating Non-repudiable Consent*, and *Handling an Emergency situation*. The *Authenticating the Patient* process is used by an SP to prevent an unauthorised person from using a patients' *Smart Phone* to access their medical information. The *Modifying an Access Control List* process is used to give the power to patients to decide who can access their medical record. The *Viewing EHRs* process is used to enable a patient to view his or her centralised *Electronic Health Record* via a *Smart Phone*. The *Identifying the Patient* procedure is used by the TTP to identify a patient when they want to request data from the TTP. The *Generating Non-repudiable Consent* procedure is used to make a patient accountable when he or she gives consent. The *Handling an Emergency* process is used to detect and inform a patient's location, and automatically call and send a patient's details to an Emergency Room.

The AD protocol is used when an *Authorised Person* (AP) such as a doctor wants to request data from, respond to, or communicate with patient's *Smart Phone* (SP) or a *Trusted Third Party* (TTP). In total the AD protocol requires seven major processes and procedures: *Authenticating an Authorised Person*, *Identifying an Authorised Person*, *Getting Consent*, *Establishing NFC Communication*, *Generating Referral Letter*, *Non-Repudiable Setup Message*, and *Verifying a Referral Letter*. The *Authenticating an Authorised Person* process is used by an AD to prevent an unauthorised person from using the AD to access the patient's medical information. The *Identifying an Authorised Person* procedure is used by a TTP to identify an AP accurately when he or she wants to have access to data from the TTP. The *Establishing NFC Communication* process is used by an AD to establish an NFC session with the SP. The *Generating Referral Letter* process is used by an AP to send a RL to a specialist. The *Non-Repudiable Setup Message* procedure is used by the AD to introduce itself to the SP. The *Verifying a Referral Letter* process is used by an AP to have access to a patient's RL from the TTP.

The *Trusted Third Party* (TTP) protocol is used when the TTP wants to request data from, respond to or communicate with the *Smart Phone* (SP) and *Authorised Device* (AD). In total the TTP protocol requires five major processes: *Establishing a SSL/TLS Session*, *Verifying a Setup Message*, *Verifying Patient Consent*, *Identifying the SP or AD*, and *Storing or Retrieving a Referral Letter*. All these processes are used to link the SP's and AD's processes and procedures.

While complex, all of these protocols can be implemented using existing technologies. Elsewhere we have modeled the protocols in ISO's Specification and Description Language and have simulated their behaviour in the UPPAAL model checker.

5 Conclusion

Ubiquitous access to a patient's medical records is an important aspect of caring for the patient. Using new technologies such as *Java SIM Cards* to address the challenges of ubiquitous access to EHRs is vital for current healthcare systems. While full EHRs

can be accessed from an *Electronic Health Records Centre* (EHRC), partial EHRs contained within a *Java SIM Card* can be used at the patient point-of-care to help quick diagnosis of a patient's problems. By taking advantage of the *Java SIM Card* and related communication and security technologies, we proposed a secure framework and communication protocols which provide a solution for ubiquitous access to EHRs without imposing any major changes on existing infrastructure.

Acknowledgments

We wish to thank the anonymous reviewers for their helpful comments.

Reference

1. Institute-of-Medicine. To err is human: Building a safer health system 2000, http://www.nap.edu/books/0309068371/html (cited September 23, 2008)
2. Abraham, C., Watson, R.T., Boudreau, M.-C.: Ubiquitous access: on the front lines of patient care and safety. Communications of the ACM 51(6), 95–99 (2008)
3. Issa, O., Gregoire, J.C., Belala, Y., James, W.: 3G Embedded Communication System for Medical Applications. In: 2nd Annual IEEE Systems Conference (2008)
4. Chenhui, Z., Huilong, D., Xudong, L.: An Integration Approach of Healthcare Information System. In: International Conference on BioMedical Engineering and Informatics (2008)
5. Bishop, B., Maloney, D., Wilson, P., Nader, N., Sembritzki, J., Meazzini, G., Morency, D.: US cards hold medical records. Card Technology Today 12(6), 14–15 (2000)
6. Chan, A.T.S., Cao, J., Chan, H., Young, G.: A web-enabled framework for smart card applications in health services. Communications of the ACM 44(9), 76–82 (2001)
7. Chang, Y.F., Chen, C.S., Zhou, H.: Smart phone for mobile commerce. Computer Standards & Interfaces 31(4), 740–747 (2009)
8. Kim, D.-K., Mehta, P., Gokhale, P.: Describing access control models as design patterns using roles. Paper Presented at the Proceedings of the, Conference on Pattern Languages of Programs (2006) (retrieved)
9. Alhaqbani, B., Fidge, C.: Access Control Requirements for Processing Electronic Health Records. In: ter Hofstede, A.H.M., Benatallah, B., Paik, H.-Y. (eds.) BPM Workshops 2007. LNCS, vol. 4928, pp. 371–382. Springer, Heidelberg (2008)
10. Kambourakis, G., Maglogiannis, I., Rouskas, A.: PKI-based secure mobile access to electronic health services and data. Technology & Health Care 13(6), 511–526 (2005)
11. Articsoft. Introduction to Public Key Infrastructure (2009), http://www.governmentsecurity.org/forum/index.php?showtopic=1630 (cited May 10, 2009)
12. The Biometric Consortium. An Introduction to Biometric (2009), http://www.biometrics.org/html/introduction.html (cited May 10, 2009)
13. ITU-T Next Generation Network. Definition of Next Generation Network (2009), http://www.itu.int/ITU-T/studygroups/com13/ngn2004/working_definition.html (cited May 10, 2009)
14. Morak, J., Hayn, D., Kastner, P., Drobics, M., Schreier, G.: Near Field Communication Technology as the Key for Data Acquisition in Clinical Research. In: First International Workshop on Near Field Communication, NFC '09 (2009)

15. Pak, T.: JAVA SIM card (2009), http://www.tele-pak.com/plastic-cards/javacards.html (cited December 23, 2009)
16. Peersman, C., Cvetkovic, S., Griffiths, P., Spear, H.: The Global System for Mobile Communications Short Message Service. IEEE Personal Communications 7(3), 15–23 (2000)
17. Hu, J.: Mobile fingerprint template protection: Progress and open issues. In: 3rd IEEE Conference on Industrial Electronics and Applications, ICIEA 2008 (2008)
18. Chin, L.-P., Chen, J.-Y.: SIM card based e-cash applications in the mobile communication system using OTA and STK technology. In: 2006 IET International Conference on Wireless, Mobile and Multimedia Networks (2006)
19. Haverinen, H., Asokan, N., Maattanen, T.: Authentication and key generation for mobile IP using GSM authentication and roaming. In: IEEE International Conference on Communications, ICC 2001 (2001)
20. Chen, Z.: Technology for Smart Cards: Architecture and Programmer's Guide 2000. Pearson, London (2000)
21. ITU-T X.210, ITU-T Recommendation X.210. Open Systems Interconnection - Basic Reference Model: Conventions for the Definition of OSI Services (1993)