Securing electronic health records with novel mobile encryption schemes

Dasun Weerasinghe*, Kalid Elmufti, Muttukrishnan Rajarajan and Veselin Rakocevic

Mobile Networks Research Group
School of Engineering and Mathematical Sciences
City University
Northampton Square
London, EC1V 0HB, UK
E-mail: dasun.weerasinghe@city.ac.uk
E-mail: k.elmufti@city.ac.uk
E-mail: r.muttukrishnan@city.ac.uk
E-mail: v.rakocevic@city.ac.uk
*Corresponding author

Abstract: Mobile devices have penetrated the healthcare sector due to their increased functionality, low cost, high reliability and easy-to-use nature. However, in healthcare applications the privacy and security of the transmitted information must be preserved. Therefore applications require a concrete security framework based on long-term security keys, such as the security key that can be found in a mobile Subscriber Identity Module (SIM). The wireless nature of communication links in mobile networks presents a major challenge in this respect. This paper presents a novel protocol that will send the information securely while including the access privileges to the authorised recipient.

Keywords: m-health; electronic health records; mobile technology; security; privacy; encryption; single-sign-on; Subscriber Identity Module; SIM; wireless.

Reference to this paper should be made as follows: Weerasinghe, D., Elmufti, K., Rajarajan, M. and Rakocevic, V. (2007) 'Securing electronic health records with novel mobile encryption schemes', *Int. J. Electronic Healthcare*, Vol. 3, No. 4, pp.395–416.

Biographical notes: Dasun Weerasinghe is a PhD research student at City University, London. His research interests include service-oriented architecture for mobile applications, security protocol development and information security in wireless networks. He holds a first-class honours BSc (Eng) degree in Computer Science and Engineering from the University of Moratuwa, Sri Lanka.

Kalid Elmufti is a PhD research student at City University, London. He has worked on various security projects, including cryptography and GSM/UMTS security. Recently he has developed security systems and protocols to address issues on authentication and privacy in mobile web services. Elmufti obtained his MSc from Imperial College, London.

Dr. Muttukrishnan Rajarajan has worked as a Network and Services Management Consultant within LogicaCMG. He has active research in mobile and wireless security with a special focus on healthcare. He has published more than 100 journal and conference papers and also chairs some conferences in the area of mobile healthcare.

Dr. Veselin Rakocevic is a Senior Lecturer at City University, London. His main research interests include management, quality of services and security of wireless networks. He is a member of IEEE and of the TPC for a number of conferences and has published over 25 papers in international journals and conferences.

1 Introduction

Nowadays, we live in the era of digital communication, digital information and digital data, where users are interested in being 'always connected', in being more nomadic and in having rapid access to information. During the recent past, initiatives have been taken both by academia and by the industries towards improving the healthcare and safety of the public by using information, communication and mobile technologies (Moran *et al*., 2007). Research activities have focused on achieving portability of medical records, monitoring real-time health status of the patients and enhancing the concept of online diagnosis and telemedicine, which deals with remote delivery of health services by means of mobile communications. In a broader sense, such healthcare applications can be termed 'm-health'. M-health is about an emerging set of applications and services that people can access from their web-enabled mobile devices (Istepanian *et al*., 2004; Dwivedi *et al.*, 2007). Consumers can use mobile devices to conduct transactions (*e.g.*, pay the consultants, buy prescriptions, send information to hospitals), access medical records and other information, and interact with database services (*e.g.*, pathology reports, ECG reports), capturing (*e.g.*, taking pictures of a skin allergy) and downloading images (*e.g.*, X-rays, ECG). In the future, it is expected that mobile technology can be used to perform most of the day-to-day activities that are being carried out today by nurses, receptionists, administrators, pharmacists and even doctors within a hospital environment (Sneha and Varshney, 2007). M-health will be an attractive solution to the already overstretched and underbudgeted health sector, since it reduces the current paper-based work, decreases waiting time, enhances healthcare services with efficient, faster and more reliable methods, eliminates errors that can occur in the paper records and speeds up administrative procedures (Wang and Du, 2005). Mundy and Chadwick (2004) have discussed some factors positively influencing the technology, efficiency, cost and current process in the UK National Health Service (NHS) for implementing the electronic transmission of prescriptions. Belsis, Dwivedi and their colleagues have also highlighted the importance of medical personnel having round-the-clock access to clinical data irrespective of the geographic location (Belsis *et al*., 2007). Another advantage of this mobile technology is that multiple personnel (*i.e.*, doctors, nurses, consultants, pharmacists, insurance providers) can access the medical records of the same patient simultaneously with role-based authorisation. The role-based authentication is vital to define the confidentiality level for patient's medical records and protect the patient's privacy (Susilo and Win, 2006). But even though the technology makes

m-health possible, many open issues still exist in the mobile healthcare environment such as security of electronic data transactions, secure mobile user authentication, efficiency of the data services and privacy safeguarding of the patient's medical records (Marti *et al*., 2004; Blobel, 2004). M-health is open to most security and privacy attacks during data transmission, such as modification of graphical images (*e.g.*, X-rays, pictures of skin allergies) or medical records that are transmitted from a patient to a doctor/laboratory. These modifications will be subjected to wrong diagnosis by the doctor, resulting in life-threatening situations. Therefore it is mandatory to employ appropriate security mechanisms to protect the medical records in m-health. These mechanisms include authentication, authorisation, integrity, access control and privacy protection.

The Wireless Application Protocol (WAP) and Short Message Service (SMS) have enabled patients and medical personnel to be in touch remotely. The WAP-based product called LifeChart enables doctors to monitor patients' conditions online and take care of their medical needs. The BBC health mobile service is a WAP-based product that provides health information to the mobile phone. WirelessMed and MedicalPlanet are two other WAP-enabled healthcare products for doctors and patients (Belsis *et al*., 2007). Researchers from the University of La Laguna have implemented a diabetes management system (Ferrer-Roca *et al*., 2004) using SMS. The existing mobile healthcare delivery based on text messaging and WAP technologies does not provide reliable message-level security for role-based authentication. Text messages are open to threats of spoofing, eavesdropping and modification of information due to the weak security protection at the Short Message Service Centre (SMSC) Gateway (Sillanpaa, 2001). The Wireless Transport Layer Security (WTLS) protocol is the security layer of WAP applications and it comes with a 40-bit DES encryption method, which is a weak encryption algorithm against brute-force attacks (Singelee and Preneel, 2005; Markku-Juhani, 1999). Susilo and Win (2006) have highlighted the importance of encrypting electronic health records in broadcast messages in their paper and they introduced a novel encryption method specifically for health records. Although WAP is a well-established protocol, it still suffers from several security flaws and hence a more reliable mechanism is needed to guarantee the privacy of medical information. In this paper the authors present a novel security protocol based on the Subscriber Identity Module (SIM) security, which can eliminate security flaws and provide a mobile environment which is reliable and secure for electronic healthcare data exchange.

Mobile web services, together with the XML-based security, present a proved framework for enterprise-level architectural schemes (MacDonald *et al*., 2006); but to the best of our knowledge, to date, there is no mobile web services model based on secure SIM authentication, XML security and role-based authentication implemented for healthcare services. This paper presents mobile web services environment based on a SIM identity, XML Encryption and XML Signature for healthcare applications. Implementation of this security model will improve the security, privacy, reliability and quality of the healthcare information exchange.

2 Mobile healthcare environment

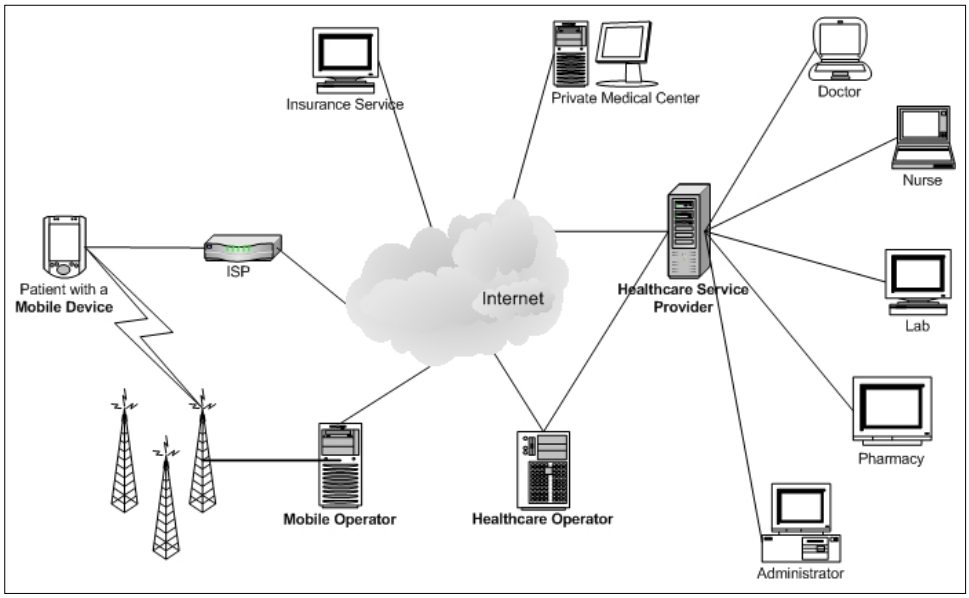
The m-health architecture allows users to use the current SIM-based authentication mechanisms from trusted domains to access a wide range of electronic service providers. This is achieved using Single-Sign-On (SSO) technologies (Hillenbrand *et al*., 2005;

Jeong *et al*., 2004) with standard authentication techniques such as the Universal Mobile Telecommunications System (UMTS) authentication system. The SSO is a technique that enables a user to authenticate once and gain access to multiple systems. To facilitate the SSO there has to be an enterprise unit to form a circle of trust by establishing business agreements, user identities and cryptographic keys with all the connected parties. In the Third Generation Partnership Project (3GPP), mobile architecture security and trust reside in the Home Location Registry (HLR) of the mobile operator and the unalterable mobile operator-issued SIM card. The subscriber identity is provided by the HLR to the third-party registered service operators to identify their users up to a certain level. The mobile operator supplies the service credentials that allow a co-located Network Application Function (NAF) (ETSI, 2005b) and Liberty-enabled Identity Provider (3GPP, 2007) entity to implement a controlled service to mobile stations from multiple trust domains. The mobile operator interacts with the system using standard and internationally agreed protocols. The proposed schema makes use of 3GPP GAA architecture (ETSI, 2005a), which is a 3GPP framework for mutual authentication of users and network applications in third-generation (3G) mobile networks (Gehrmann *et al*., 2001). It describes the usage of a single authentication infrastructure for all the services, assuming the existence of service-level agreements between service providers and the network operators. Services are available to the mobile station from various and disparate trust domains and capable of being set up using Over-The-Air techniques (MacDonald *et al*., 2005). The solution provided in this environment uses a single SIM card and makes use of the existing security mechanisms within the UMTS infrastructure (ETSI, 2005a). It authenticates the user based on the long-term credentials present in the mobile SIM and the security of the GAA lies in the assumption that the access to that long-term shared secret is difficult. The SIM security keys will be used to generate tokens that can be used to authenticate the mobile station with the mobile operator once and, using the credentials issued by the mobile operator, the mobile station can carry out 'multiple' m-health transactions with several Healthcare Service Providers (HSP) with or without disclosing their identities (MacDonald *et al*., 2006).

A patient with a mobile device connects with HSP in a mobile environment. The mobile device has a SIM card in it and it connects with a mobile operator. The mobile environment also includes the service providers that provide healthcare service to patients such as HSP, insurance service providers and private medical centres. All the service providers are registered with the Healthcare Operator (HO). The HO authorises and authenticates mobile devices for accessing service providers. The patient has to be authenticated by the HO before accessing services at service providers. It is assumed that the patient is registered with the service providers before requesting services and service providers identify the patient using the identity provided by the HO. The HSP is assumed to be a trusted entity. It has a set of stakeholders such as a doctor, nurse, lab, pharmacy and administrator to provide the healthcare services and they are all connected to the intranet of the HSP. The HSP defines different access control levels to each stakeholder for accessing the healthcare information. The patient with the mobile device communicates with the mobile operator over the UMTS network. The communication between the HO and the service provider takes place over the internet or using a dedicated network link. The mobile device communicates with the service providers and the HO through the mobile operator or over the internet.

The mobile healthcare architecture has four types of main actors: the patient with a mobile device, the mobile operator, the healthcare operator/identity provider and the service provider. The patient accesses the services via a bandwidth-constrained mobile station, comprising the mobile device and service-enabling SIM card connected to a mobile operator over the UMTS network. The HO is connected to registered service providers such as the HSP, a private medical centre and insurance service providers to provide healthcare services to patients. The patient is authenticated by the HO using the SIM credentials at the mobile operator. Once successfully authenticated with the HO, the patient can request access to the services at service providers. The implementation of all the service providers and the HO is based on Service-Oriented Architecture (Coetzee and Eloff, 2004; Beznosov *et al.*, 2005). Service providers communicate with the patient and the mobile operator using the Hypertext Transfer Protocol (Sun Microsystems, 2003). The architecture uses some of the latest XML encryption, XML signature and XML Key Management technologies, which are much faster and consume less power for secure mobile applications.

Figure 1 Mobile healthcare network



3 Security requirements

Healthcare information should be protected from security vulnerabilities when it is transmitted in the mobile environment. Wickramasinghe and Misra (2004) have mentioned six key aims in order to achieve high-quality healthcare. To the authors' knowledge there are currently no security and privacy standards for mobile healthcare in Europe. In general, the following are the security and privacy challenges open in the mobile healthcare environment:

- The access to the healthcare applications should be restricted only to the authorised persons with the use of cryptographic mechanisms and secure private tokens like smart cards. Usernames and passwords are not sufficient for such an operation, since they can easily be hacked, revealed or lost. Strong authentication is thus required.
- The patient's mobile device should be prevented from unauthorised transactions if an unauthorised party tries to masquerade as an HSP.
- The patient's health information is transmitted through the mobile operator and the internet. The communication should be encrypted, so that it disables eavesdroppers from getting in the channel and modifying or reading data without authorisation.
- Messages in the above environment consist of the patient's sensitive and critical health information. Therefore messages should be protected from man-in-the-middle attacks.
- Stakeholders in the HSP respond to the patient's healthcare requests. There must be clear proof that a message was actually created by the specified stakeholder; otherwise, it would be possible for unauthorised persons to create invalid messages using an authorised name. For example, if a doctor prescribes medication using the mobile environment, the message should have the same legal bindings as if it were handwritten by the doctor (Wickramasinghe and Misra, 2004). Further to this, each stakeholder should be responsible for the messages that are sent to patients and the sender's identification should be available on the message. Therefore digital signature mechanisms should be incorporated to ensure document integrity and nonrepudiation.
- It is necessary to register the date and time of the message creation at the healthcare services, as the senders' proof of in-time diagnosis and treatment for certain patients.
- Once a patient requests a healthcare service, the patient's health information is received by the HSP and that information is manipulated among the stakeholders of the HSP. The patient's full health information should not be visible to all the stakeholders; only the required part of the messages should be passed on to them. So the role-based access control mechanism should be implemented to maintain the confidentiality of the patient's health information. Meanwhile, external service providers like health insurance companies need to access the patient's medical records to provide insurance coverage. These external parties should be able to access only the specific information they are looking for and the patient's privacy has to be protected from external access.
- Stakeholders are allowed only to add information to the health record message, without any authority to view or change previously added information.
- There should be a process of tracking all the changes and user access to the patient's health record message.

4 Protocol

The protocol presented in this paper provides secure authentication and XML-based security between patients and healthcare services over a mobile network. Healthcare information is transmitted securely in the network and unauthorised users are unable to access those data. The privacy of the healthcare data is protected since the HSP defines role-based access control rules for the messages. The protocol is derived using the UMTS authentication, SSO and XML security technologies. The protocol addresses authentication, data integrity, confidentiality, nonrepudiation, data access control and privacy of healthcare information in the mobile healthcare environment. Communication messages are in XML format and communication is based on the Simple Object Access Protocol (SOAP) (Snell *et al*., 2002; Lai *et al*., 2005). The protocol can be separated into the following three phases.

4.1 Phase 1: Mobile station obtains authentication from the healthcare operator

The patient with the mobile station obtains authentication from the HO, using the SIM authentication at the mobile operator. The sequence of exchanged messages (Figure 2) is as follows:

1 The patient requests access to the health services from the HO, attaching the IP Multimedia Private Identity (IMPI) number with the request.

2 If the patient has not been authenticated at this stage, the HO sends a request to the patient to initiate the Bootstrapping Procedure (BSP).

3 The patient initiates the BSP at the Mobile Operator.

4 The patient obtains the B-TID, which is a string of base-64 random data, the Bootstrapping Function (BSF) server domain name and the lifetime of the B-TID. The patient generates the key material (Ks) using the B-TID, which is used for secure communication between the HO and the patient.

5 The patient starts the log-in procedure by forwarding the B-TID to the HO.

6 The HO sends the B-TID to the mobile operator to obtain the relevant Ks.

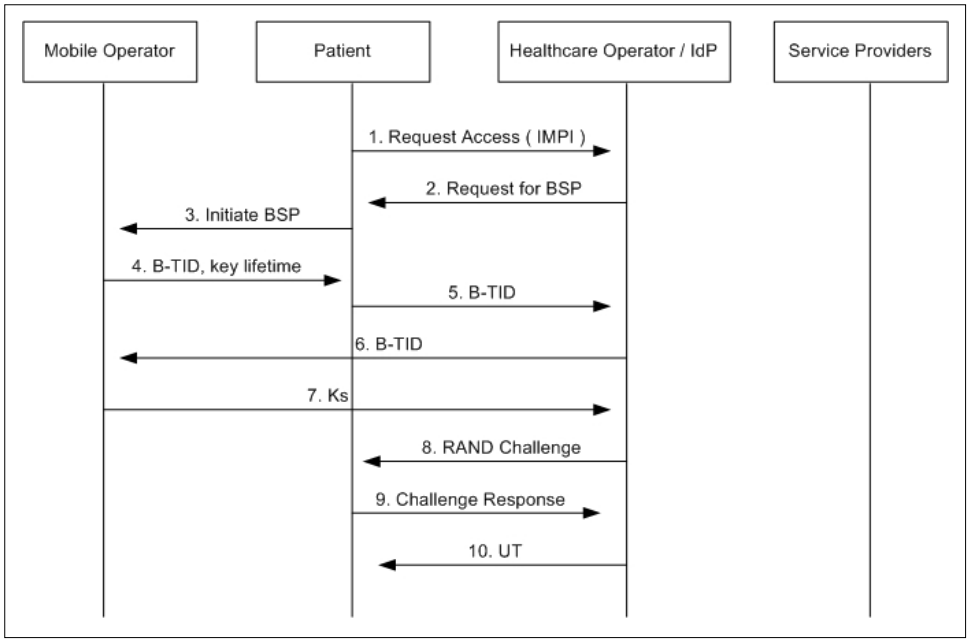
7 The HO obtains the Ks that belongs to the B-TID.

8 The HO generates a random number and sends it to the patient. The random number is used to challenge the patient's ownership of the Ks.

9 Once the patient receives the random number, the Challenge Response is generated and sent to the HO. The Challenge Response is a function of the random number and the Ks.

10 If the Challenge Response is successful, the HO generates and sends the User Token (UT) to the patient, unless it repeats Step 6. UT is user identification with a timestamp and the content of the UT is encrypted using the Ks.

Figure 2 Mobile station obtains authentication from the healthcare operator



4.2 Phase 2: Mobile station obtains authentication from the service provider

Before requesting a service from a service provider, a patient has to be authenticated by the HSP. Refer to Figure 3. The steps are as follows:

1 Once the UT is received, the patient can access service providers who are registered with the HO. The patient requests the access to an HSP from the HO by sending the SP identity (SPID) and the UT.

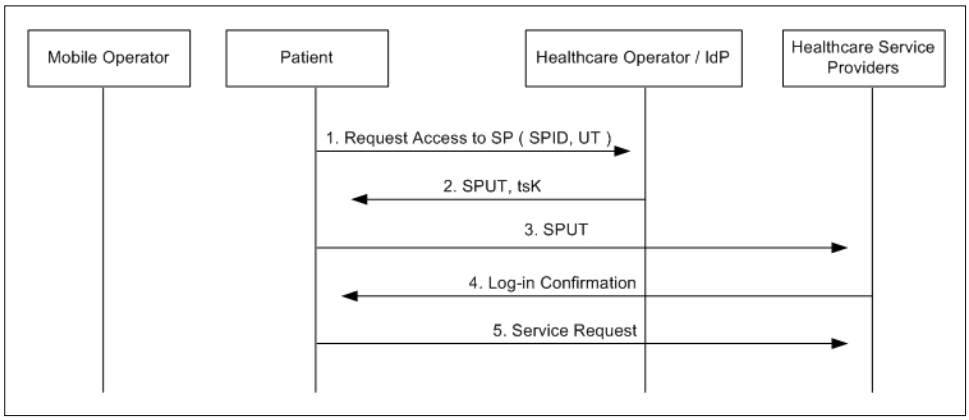
2 The patient receives the Service Provider User Token (SPUT) and the Temporary Session Key (tsK) from the HO and the response message is encrypted by Ks. The SPUT consists of SPID, tsK, timestamp (TS) and the patient's identification at HO with the HSP. This token is digitally signed by the HO and encrypted using the public key of the HSP.

3 The patient sends the SPUT to the HSP and initiates the communication.

4 If the SPUT is extracted and verified successfully, the HSP sends the log-in confirmation to the patient. Otherwise, a failure message is sent and the patient has to request a new SPUT from the HO.

5 After obtaining successful confirmation, the patient sends the service request to the HSP with the healthcare information. The information is embedded in the message in an XML format and the message is encrypted using the tsK.

Figure 3 Mobile station obtains authentication from the healthcare service provider



4.3 Phase 3: Data access level in healthcare service provider

A single XML document with the patient's health information is manipulated among all the stakeholders at the HSP but different access levels are defined for the data access in the document. This can be explained using a scenario where a patient sends a blood pressure count to the HSP and obtains the healthcare service from different stakeholders in the HSP.

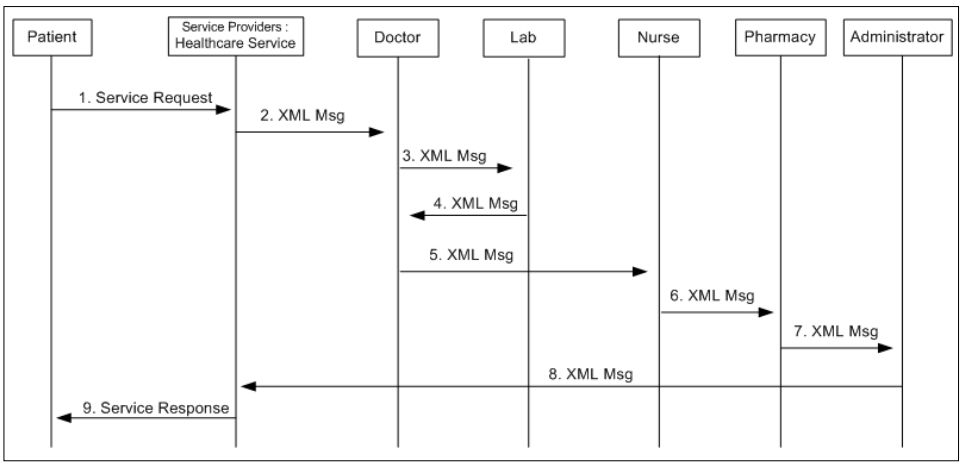
- The patient initiates the access to the HSP and sends the service request. The request message is encrypted using the tsK and the service request XML is concatenated with the request type, the request-receiving party, the patient's information and the health information. In this scenario the patient requests a medication from a doctor while sending the blood pressure count. So the HSP receives the message containing the request type as medication and the receiving party as the doctor. The HSP should then send the health information to the relevant doctor and the patient's information to the healthcare administrator. Since the HSP manipulates the same XML document to all the user levels, both parties are looking into the same XML document but the health information should not be visible to the administrator, neither should the financial information be visible to the doctor. Therefore the XML element in the document, that contains health information including the timestamp, is encrypted using the doctor's public key and the financial information is encrypted using the administrator's public key. The timestamp is generated by the HSP. Before the encryption, both of the XML elements are digitally signed using the private key of the HSP for the authentication and it is forwarded to the doctor for the medication process.
- Once the doctor receives the XML document, it decrypts the XML data elements that were encrypted using its public key and verifies the XML signature using XML and SIM security to provide role-based authentication and encryption in mobile healthcare for the authentication. However, the doctor is unable to access the financial information that is concatenated in the same XML document.

- Let us assume the doctor requires some laboratory results based on the patient's blood pressure count. The doctor appends a new XML element to the document that includes the health data readings of the patient and the timestamp. The new XML element should only be extracted by the laboratory. Therefore the doctor signs the XML element for integrity and encrypts it using the public key of the lab.
- Once the lab receives the XML document, it decrypts the XML element using its own private key and verifies the sender from the signature. Then the laboratory results and the timestamp are embedded in the XML document, signed by the private key of the lab and then encrypted using the doctor's public key. So the lab result can be viewed only by the doctor.
- The doctor receives the XML document, decrypts the XML data element that was appended by the lab, verifies the lab's XML signature and extracts the laboratory results. Then the doctor embeds new XML elements to the document such as listed below and each XML element has instructions and information for specific users, including the timestamp.
    a An XML element to the nurse is signed by the doctor and it is encrypted using the public key of the nurse.
    b An XML element to the pharmacy is signed by the doctor and it is encrypted using the public key of the pharmacy.
    c An XML element to the patient is signed by the doctor and it is encrypted using the HSP public key. Once all the XML elements are appended successfully, the document is forwarded to the nurse.
- The nurse is allowed to view only the XML elements that are encrypted using his/her public key. The XML signature of the element is verified for the authentication of the message. Let us assume that the nurse is required to send a message to the patient. So the nurse may include a new XML message and timestamp elements in the XML document with the digital signature and encrypts the XML element using the HSP public key.
- Once the pharmacy receives the XML document, it decrypts the XML messages that were appended by the doctor about medicines and it may append XML messages to the administrator for invoicing the patient, with digital signature and message encryption.
- The XML document is finally received by the administrator of the HSP. The administrator extracts the patient's information that was appended by the HSP and other XML elements that were encrypted using its public key. The administrator embeds the invoice and other financial information on the patient into the XML document, signs it using his/her private key and encrypts it using the HSP public key. Then the XML document is sent to the HSP. An example of an XML document that is sent to the HSP is shown in Appendix C.
- Once the HSP receives the document, it decrypts all the XML messages that were encrypted using its own public key and verifies the senders with XML signatures. These messages contain medication and financial information for the patient;

therefore the HSP appends all the decrypted XML data elements in the messages, encrypts the complete message and the timestamp using the tsK and sends them to the patient.

- Once the patient receives the message, he/she decrypts it using the tsK and views the medication information in the XML document. Each XML element consists of the XML signature of the sender and the patient can verify those signatures using the XML key management feature in the HSP.

Figure 4 Data access levels in the healthcare service provider



The HSP maintains a single XML document for each patient's request and it contains requests and information for many stakeholders. The information access control levels should be maintained for the data in the XML document since the same document is transferred between different user levels concatenating all the information. The XML document contains separate XML elements for different user levels and each XML element is encrypted using the user's public key. However, the information in certain XML elements may be referred to by more than one user level in the system. Therefore, advanced XML Encryption features such as partial encryption and multiple encryption are used to implement the information access control.

During the XML document manipulation, stakeholders may append information to the document and that information should be authenticated using the XML Signature of the stakeholder. Since for each signature in the message, the respective stakeholder is responsible, the appended message and the sender can be verified on each message.

The HSP generates separate key pairs for each user in the system, saves a copy in the HSP and installs it in the user's applications or devices. It also provides XML Key Management service to process the key information related to the XML Signature and the XML Encryption.

The same XML document is used to send information to service providers such as insurance services and private medical centres that are interested in the patient's health information. The HSP appends information required for those parties in the XML document, signs the information using the HSP's private key and encrypts it using the receiver's public key. So the receiver can only view the message that was encrypted

using his/her own public key and the message can be verified using the sender's signature. As an example, the patient may send the same XML document to the insurance provider to claim the medical insurance. The insurance provider will be able to retrieve only the invoice details from the document but not the patient's health information.

5 Security analysis

Several security threats exist in the mobile healthcare environment. This section will discuss the possible security issues and the solutions provided by the protocol defined in this study.

5.1 Message confidentiality

The communication between the patient and the mobile operator is secured using symmetric encryption. Confidentiality for the UMTS air interface is based on a long-term secret key, shared by the SIM in the patient's mobile device and the mobile operator. The communication between the patient and the HO is based on symmetric encryption using the shared session key that is generated at the mobile operator and the patient's mobile device. The mobile operator transfers the generated session key to the HO in an established secure channel between the mobile operator and the HO. A secured confidential communication channel is established between the healthcare operator and the patent's mobile device based on the symmetric encryption and the patient uses the secure channel for the authentication with the HO and transfer-sensitive data. Therefore, the sensitive data that is communicated between the patient and the HO is protected from eavesdroppers. The communication between the patient and service providers is protected using the asymmetric key encryption. Service providers and stakeholders among the service providers have a pair of public and private keys for message confidentiality. Key management is a service provided by the healthcare operator to provide key pairs for registered patients and public keys for message encryption. Each communication message between patients and service providers/stakeholders is encrypted using the receiver's public key and only the receiver with the correct corresponding private key can view the message. Therefore all the patient's sensitive health records are protected from eavesdroppers and the patient's privacy is protected.

5.2 User authentication

The patient is authenticated by the mobile operator using SIM-based authentication and is authenticated by the HO based on his/her authentication with the mobile operator. The patient's mobile device has to extract the IMPI from the SIM in the mobile device and send that information to the HO for authentication. The IMPI is a unique identifier for the mobile operator and the patient's mobile device. Hence attackers are unable to get authorisation from the HO and access health records unless using a stolen SIM card or cloned SIM cards. The SIM attack can be prevented by having a PIN-protected SIM card or combining the SSO mechanism with another authentication method, *e.g.*, username and password or pin number. The patient obtains authentication from the service providers using the unique SPUT that is generated at the HO for each service access request from the patient. The patient does not have to enter any user credentials since the

authentication is based on the SSO mechanism. These authentication methods at the HSP and the HO are transparent to the user; it can be repeated whenever appropriate. The service providers with high-risk health services may combine the SSO mechanism with another authentication method to provide some extra security to the sensitive information.

5.3 User authorisation

Once the patient has been authenticated with the mobile operator, he/she is authorised to access the mobile operator to execute the bootstrapping procedure. The mobile operator authorises the patient to access the HO by returning the B-TID. The challenge response mechanism at the HO is used to authorise the patient and issue the UT. The UT is a property of the HO and it is used to authorise the patient for further communication with the HO. The patient is authorised by the HSP using the SPUT generated by the HO and patients acquire the SPUT once they have been successfully authenticated with the HO. The patient has to request each service with the appended SPUT in the message content. The HSP initiates the service after the SPUT has been validated.

5.4 Message integrity

The digital signature is used to protect the integrity of sensitive healthcare data that is communicated in the proposed architecture between patients and service providers. All the messages are digitally signed by the sender's private key and the receiver should validate the message beside the sender's public key. Therefore, the protocol protects sensitive health communication from man-in-the-middle attacks. For example, eavesdroppers are unable to change the patient's blood pressure count in a medication request to a doctor.

5.5 Message nonrepudiation

The digital signature is used to protect the sensitive messages between patients and service providers from man-in-the-middle attacks. Therefore all the sensitive messages are signed by the sender's private key. The digital signature proves that the originator had sent the message, so the healthcare stakeholders are responsible for the services provided to patients. For example, the doctor cannot deny his responses to the patient later.

5.6 Replay attacks

The authentication and authorisation messages in the architecture consist of timestamps to prevent replay attacks. An eavesdropper could capture the log-in request message of a previous protocol between a patient and an HSP. The attacker might later replay that message to try to impersonate the patient to the HSP. The attack will not succeed if the HSP validates the timestamp of the request message. The user tokens such as UT and SPUT are generated at the HO and contain the timestamp and lifetime of the token. These tokens are integrity protected and attackers are unable to alter the timestamps before the attack.

5.7 Access control

The HSP consists of many stakeholder and patient's health-sensitive messages are populated among them to provide services. To protect the patient's privacy, it is critical that only the authorised stakeholders are able to view the messages, and the stakeholder should not be able to view the full message, but only the authorised section of the message. The messages in the proposed architecture are encrypted using partial encryption and only the authorised parties with the right cryptographic keys are allowed to decrypt the full message or part of the message. For example, the laboratory should not see the doctor's comments on the patient's health. The patient's privacy is protected using the role-based access control on the healthcare messages.

6 Conclusion

With the rapid growth in mobile technology and digital communication, users prefer to have real-time access to healthcare services over the mobile phone. M-health is an attractive solution for the healthcare sector since it reduces paper-based work, minimises the costs, decreases the waiting time for appointments, speeds up the medication process and increases the reliability and quality of health services. The increasing usage of mobile handsets by all ages and extra features that are available in today's handsets make the delivery of healthcare data using mobile technology a reality. However, as healthcare data is sensitive, it has to be protected against unauthorised access. The mobile healthcare environment and protocol discussed in this paper provides a secure solution to m-health using the SSO, SIM security and mobile web services technologies. Meanwhile, role-based authentication is provided to validate this novel protocol in the healthcare environment. The m-health solution proposed in this study provides security mechanisms such as confidentiality, authentication, authorisation, integrity, nonrepudiation and access control. The proposed architecture will also give improved reliability compared to other existing m-health solutions based on text messaging and WAP technologies.

References

Belsis, M.A., Dwivedi, A.N., Gritzalis, S., Bali, R.K. and Naguib, R.N.G. (2007) 'Providing secure mAccess to medical information', *International Journal of Electronic Healthcare*, Vol. 3, No. 1, pp.51–57.

Beznosov, K., Flinn, D.J., Kawamoto, S. and Hartman, B. (2005) 'Introduction to web services and their security', *Information Security Technical Report*, Vol. 10, pp.2–14.

Blobel, B. (2004) 'Authorisation and access control for electronic health record systems', *International Journal of Medical Informatics*, Vol. 73, No. 3, pp.251–257.

Coetzee, M. and Eloff, J.H.P. (2004) 'Towards web service access control', *Computers and Security*, Vol. 23, pp.559–570.

Dwivedi, A., Wickramasinghe, N., Bali, R.K., Naguib, R.N.G. and Goldberg, S. (2007) 'Critical success factors for achieving superior m-health success', *International Journal of Electronic Healthcare*, Vol. 3, No. 2, pp.261–278.

European Telecommunications Standards Institution (ETSI) (2005a) *Access to Network Application Functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS): Generic Authentication Architecture*.

European Telecommunications Standards Institution (ETSI) (2005b) *Generic Bootstrapping Architecture (GBA)*.

Ferrer-Roca, O., Cardenas, A., Diaz-Cardama, A. and Pulido, P. (2004) 'Mobile phone text messaging in the management of diabetes', *Journal of Telemedicine and Telecare*, Vol. 10, No. 5, pp.282–285.

Gehrmann, C., Horn, G., Jefferies, N. and Mitchell, C.J. (2001) 'Securing access to mobile networks beyond 3G', *Proceedings of the IST Mobile Communications Summit*, Barcelona, Spain, September, pp.844–849.

Hillenbrand, M., Gotze, J., Muller, J. and Muller, P. (2005) 'A single-sign-on frame work for web-services-based distributed applications', *Proceedings of the 8th International Conference on Telecommunications, ConTEL 2005*.

Istepanian, R.S.H., Jovanov, E. and Zhang, Y.T. (2004) 'Guest editorial and introduction to the special section on m-health: beyond seamless mobility and global wireless health-care connectivity', *IEEE Transactions on Information Technology in Biomedicine*, Vol. 8, No. 4, pp.405–414.

Jeong, J., Shin, D. and Shin, D. (2004) 'An XML-based security architecture for integrating single-sign-on and rule-based access control in mobile and ubiquitous web environments', *EUC2004, LNCS 3207*, pp.903–913.

Lai, K.Y., Phan, T.K.A. and Tari, Z. (2005) 'Efficient SOAP binding for mobile web services', *Proceedings of the IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05)*, pp.2–14.

MacDonald, J., Elmufti, K., Weerasinghe, D., Rajarajan, M., Rakocevic, V. and Khan, S. (2006) 'A web services shopping mall for mobile users', *The 4th IEEE European Conference on Web Services (ECOWS'06)*, Switzerland.

MacDonald, J., Sirett, W.G. and Mitchell, C.J. (2005) 'Overcoming channel bandwidth constraints in secure (SIM) applications', *Security and Privacy in the Age of Ubiquitous Computing*, Springer Science and Business Media, pp.539–549.

Markku-Juhani, O.S. (1999) 'Attacks against the WAP WTLS protocol', *Proceedings of the IFIP TC6/TC11 Joint Working Conference on Secure Information Networks*, Deventer, Netherlands, Vol. 152, pp.209–215.

Marti, R., Delgado, J. and Perramon, X. (2004) 'Network and application security in mobile e-health applications', *Lecture Notes in Computer Science*, Vol. 3090, pp.995–1004.

Moran, E.B., Tentori, M., Gonzalez, V.M., Favela, J. and Martinez-Garcia, A.I. (2007) 'Mobility in hospital work: towards a pervasive computing hospital environment', *International Journal of Electronic Healthcare*, Vol. 3, No. 1, pp.72–89.

Mundy, D. and Chadwick, D.W. (2004) 'Electronic transmission of prescriptions: towards realising the dream', *International Journal of Electronic Healthcare*, Vol. 1, No. 1, pp.112–125.

Sillanpaa, A. (2001) 'Mobile asset security and how to make money on it', *T-110.501 Seminar on Network Security*, Publications in Telecommunications and Multimedia, TML-C7.

Singelee, D. and Preneel, B. (2005) 'The wireless application protocol', *International Journal of Network Security*, November, Vol. 1, No. 3, pp.161–165.

Sneha, S. and Varshney, U. (2007) 'A wireless ECG monitoring system for pervasive healthcare', *International Journal of Electronic Healthcare*, Vol. 3, No. 1, pp.32–50.

Snell, J., Tidwell, D. and Kulchenko, P. (2002) *Programming Web Services with (SOAP)*, O'Reilly, June.

Sun Microsystems (2003) 'Sun Java wireless toolkit', Version 2.1, http://java.sun.com/products (accessed April 2003).

Susilo, W. and Win, K.T. (2006) 'Securing electronic healthcare records with broadcast encryption schemes', *International Journal of Electronic Healthcare*, Vol. 2, No. 2, pp.175–184.

Third Generation Partnership Project (3GPP) (2007) 'Interworking of liberty alliance ID-FF, ID-WSF and generic authentication architecture', *3GPP TR 33.980*, Version 1.0.0, Release 4.

Wang, J. and Du, H. (2005) 'Setting a Wireless Local Area Network (WLAN) for a healthcare system', *International Journal of Electronic Healthcare*, Vol. 1, No. 3, pp.335–348.

Wickramasinghe, N. and Misra, S.K. (2004) 'A wireless trust model for healthcare', *International Journal of Electronic Healthcare*, Vol. 1, No. 1, pp.60–77.

Appendix A XML encryption

The patient's blood pressure count in a plain XML document:

<?xml version="1.0" encoding="utf-8"?>

<HealthInfo>

<Name>Ian Denley</Name>

<Bloodpressure>132</Bloodpressure>

</HealthInfo>

The patient's blood pressure count is encrypted using the partial XML encryption.

<?xml version="1.0" encoding="utf-8"?> <HealthInfo>

<Name>Ian Denley</Name>

<EncryptedData Type=http://www.w3.org/2001/04/xmlenc#Element
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:KeyName>Ian Denley</ds:KeyName>

</ds:KeyInfo>

<CipherData>

<CipherValue>DEADBEEF</CipherValue>

</CipherData>

</EncryptedData>

</HealthInfo>

Appendix B XML signature

The patient's blood pressure count is signed by XML Signature using the patient's private key.

<?xml version="1.0" encoding="utf-8"?>

<HealthInfo>

<Name>Ian Denley</Name>

<Bloodpressure id="bloodPressureReading">132</Bloodpressure>

</HealthInfo>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

<SignedInfo>

<CanonicalizationMethod

Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>

<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
<Reference URI="#bloodPressureReading">
<Transforms>
<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
<KeyInfo>
<KeyValue>
<DSAKeyValue>
<P>dsr23DS32fd</P>
<Q>jkd55ss65</Q>
<G>hdf87aaHF</G>
<Y>dfa4Jsw83</Y>
</DSAKeyValue>
</KeyValue>
</KeyInfo>
</Signature>

Appendix C Secured XML document

<?xml version="1.0" encoding="utf-8"?>
<HealthInfo>
<Name>Ian Denley</Name>
<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:KeyName>HSP_Doctor</ds:KeyName>
</ds:KeyInfo>
<CipherData>
<CipherValue id="bloodPressureReading">DEADBEEF</CipherValue>
</CipherData>

```
</EncryptedData>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
<Reference URI="#healthinfotodoctor">
<Transforms>
<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
<KeyInfo>
<KeyValue>
<DSAKeyValue>
<P>dsr2sdf3dsffd</P>
<Q>jksd33ss65</Q>
<G>hd4FsaHF</G>
<Y>dfa4Jsw83</Y>
</DSAKeyValue>
</KeyValue>
</KeyInfo>
</Signature>
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:KeyName>Doctor_Lab</ds:KeyName>
</ds:KeyInfo>
<CipherData>
<CipherValue id="bloodPressureReadingForLab">HFYSOSJSYSB</CipherValue>
</CipherData>
</EncryptedData>
</HealthInfo>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
```

<SignedInfo>
<CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
<Reference URI="#bloodPressureReadingForLab">
<Transforms>
<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>j6lw0vKtxVu83rvEPOeVu8nk=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>MC0Chs=+asHJSsaFFrVLtRlk=...</SignatureValue>
<KeyInfo>
<KeyValue>
<DSAKeyValue>
<P>dsr23DSssaFsa32fd</P>
<Q>jkd55ss65</Q>
<G>hdf87asa4aHF</G>
<Y>dfa4Jsw83</Y>
</DSAKeyValue>
</KeyValue>
</KeyInfo>
</Signature>
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:KeyName>Lab_Doctor</ds:KeyName>
</ds:KeyInfo>
<CipherData>
<CipherValue id="bloodPressureResults">HFYSOSJSYSB</CipherValue>
</CipherData>
</EncryptedData>
</HealthInfo>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod

Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
<Reference URI="#bloodPressureResults">
<Transforms>
<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>j6lw09sKSsdk00vEPOeVu8nk=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>MC0Chs=+asHJDSalsdlVLtRlk=...</SignatureValue>
<KeyInfo>
<KeyValue>
<DSAKeyValue>
<P>dsr2sdhsda32fd</P>
<Q>jkdsdksl5</Q>
<G>hdf8dsjs928F</G>
<Y>dfaKdsi0w3</Y>
</DSAKeyValue>
</KeyValue>
</KeyInfo>
</Signature>
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:KeyName>Lab_Doctor</ds:KeyName>
</ds:KeyInfo>
<CipherData>
<CipherValue id="bloodPressureResults">HFYSOSJSYSB</CipherValue>
</CipherData>
</EncryptedData>
</HealthInfo>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>

```
<Reference URI="#bloodPressureResults">
<Transforms>
<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>j6lw09sKSsdk00vEPOeVu8nk=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>MC0Chs=+asHJDSalsdlVLtRlk=...</SignatureValue>
<KeyInfo>
<KeyValue>
<DSAKeyValue>
<P>dsr2sdhsda32fd</P>
<Q>jkdsdksl5</Q>
<G>hdf8dsjs928F</G>
<Y>dfaKdsi0w3</Y>
</DSAKeyValue>
</KeyValue>
</KeyInfo>
</Signature>
```