XML Security based Access Control for Healthcare Information in Mobile Environment
Dasun Weerasinghe, Kalid Elmufti, M Rajarajan and Veselin Rakocevic
Mobile Networks Research Group
School of Engineering and Mathematical Sciences
City University,
Northampton Square, London, EC1V 0HB, UK.
abbp075@city.ac.uk

Abstract—Mobile and wireless devices have penetrated the health care sector due to their increased functionality, low cost, high reliability and easy-to-use nature. However, in such health care applications the privacy and security of the transmitted information must be preserved. Also different personal involved in the healthcare industry must have different access privileges to the patient information. In this paper we present a protocol that will share the information securely to the intended recipient using the XML encryption and XML signature technologies.

I. INTRODUCTION
This paper proposes a protocol for XML based security between a patient and the health services that builds upon a mobile communication environment. The proposed schema allows health services to provide a trusted and secure environment for healthcare information and medication management over the mobile devices. Patient is able to send the healthcare data over the mobile device to the healthcare service, healthcare service process and manipulate those data over different stakeholders in the system and finally deliver the physical or digital medications to the patient.

Mobile healthcare will be an attractive solution for the already overstretched and under budgeted health sector since it reduces current paper based work, decreases waiting list for appointments, enhances healthcare services with faster and more reliable methods, and speeds up administrative functionalities. However the use of mobile communication in healthcare has a serious security risk due to the fact that any modification, exposure to unauthorized access or loss of the healthcare data may even put human life at a risk. Therefore confidentiality, authentication, integrity and non-repudiation in healthcare data are essential for mobile healthcare. Meanwhile healthcare service defines different user levels such as doctor, nurse, laboratory, pharmacy and administrator and each level should have access different access control to healthcare data in the system.

Mobile Web services together with XML-based security present a proved framework for enterprise-level architectural schemes [8] but still there are no XML security based mobile communication models for healthcare services. Implementation of the XML Security model will improve the quality, reliability and security of the health services. In this paper we present an XML encryption and signature based mobile web services environment for health care application.

II. TECHNICAL OVERVIEW
XML is an extensible markup language specified by W3C (World Wide Web Consortium) [4]. It has become very popular quickly in data transmission because of its flexibility and the platform-independency. As the XML becomes the most popular data transmission media over the internet, a greater importance is placed on security technology for the data in XML format [9]. Confidentiality, integrity, authentication and non-repudiation are some of the security threats associated with XML data transmission.

A. XML Encryption
XML Encryption is an encryption technology that provides end-to-end security for applications that require secure transmission of XML data. It solves the security problems such as confidentiality, integrity and authentication. Further to this XML Encryption provides advanced features [5] such as

- Partial encryption: encrypts XML data within specific tags
- Multiple encryption: encrypts XML data multiple times using different keys
- Complex encryption: encrypt particular portion of the XML tags according to the designation of the recipient

Example of XML Encryption is shown in the Appendix A: let us assume, XML document contains patient’s blood pressure reading and it has to be encrypted before transmission over the Internet. Encrypted <BloodPressure> element structures with the <EncryptedData> element and it has child elements such as the <EncryptionMethod> element; contains information about encryption algorithm, the <KeyInfo> element; contains information about the decryption key, and the <CipherData> element; contains the cipher data.

B. XML Signature
XML Signature is an electronic signature technology which is defined to be used in XML data transmission. XML Signature specification [6] defines electronic signature formats using XML, the creation of electronic signature and rules for the verification process. It solves security problems such as authentication, integrity and non-repudiation. Further to this XML Signature provides advanced benefits such as
• Partial Signature; allows only data contained in specific tags to be signed in the XML document
• Multiple signature; enables multiple electronic signatures to be included in the XML document

Example of XML Signature is shown in Appendix B: Let us assume patient’s blood pressure count has to be signed before the transmission. XML signature is a document structured with the <Signature> element as the root element of the signature. It consists of child elements such as <SignedInfo> element; contains reference to the algorithm used for the XML signature creation and to the location of signed XML data that is stored, <SignatureValue> element; contains the signature value, and the <KeyInfo> element that contains the public key certification information for signature verification. The <SignedInfo> element may contain multiple <Reference> and it enables any number of XML data segments to be signed.

XML 1.0 specification has the flexibility to represent equivalent contents in multiple XML formats such as attribute occurrence sequence, blank character handling, etc [4]. The same XML document can be represented in different formats and those are different in byte representation. XML signature is a technology based on hash calculation that applies to byte representations of data. Therefore the flexibility of the XML 1.0 specification could raise critical problems in electronic signatures. To overcome this problem before the XML data is signed or verified, it is converted to a Canonical form that complies with the Canonical XML specification to ensure that the problem of format variations can be solved in order to allow the use of XML signature [2]. When signed XML data is added to a child element of another XML document and converted in accordance with the Canonical XML specification, the naming space of the added XML data changes because of canonicalization. This will lead to failure in XML signature verification when signed XML data is embedded in a SOAP message. To avoid this problem, the exclusive XML Canonicalization was established as a specification that is based on Canonical XML and excludes naming space and other contexts for the target of canonicalization [3].

C. XML Key management specification

The XML Key Management Specification (XKMS) provides an interface between XML applications and a Public Key Infrastructure (PKI) and also it specifies protocols for distributing and registering public keys [7]. This specification eliminates the complex PKI application logic implementation at the client side and allocates trust processing decisions in to separate trust processors. XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS) are two major subparts of the XKMS [1].

X-KISS defines protocols to eliminate full or partial key information processing associated with XML signature and XML encryption at the client end. The client verifies the digital signature by passing the corresponding key information to the trusted server and the server responds with the validity of the signed data. X-KRSS defines protocols to support the registration of a public key and additional data at the trusted server. Key pair may be generated at the client end or by the trusted server. This specification further defines automatic PKI renewal process without the client’s interaction, revoke key binding, private key recovery when an end user lost their private key and roaming when an end user required to use the private key in another device.

III. MOBILE HEALTHCARE ARCHITECTURE

The Mobile Healthcare architecture has four main actors; the Patient, the Mobile Operator, the Healthcare Operator and the Service Provider. The patient is assumed to access the services via a bandwidth-constrained Mobile Station, comprising the mobile device and service-enabling SIM card connected to a GPRS or UMTS mobile network. The Healthcare Operator is assumed to require the maximum number of patients for the available services, and the maximum number of available services for the participating patients. Service Providers and Patients should be capable of dynamically and asynchronously entering and leaving the system. The services should be available to patients from various and disparate trust domains and capable of being setup using Over The Air (OTA) techniques. The Mobile Operator interacts with the system using the standard and internationally agreed protocols. Healthcare Service is a service provider who is attached to the Healthcare Operator and it defines different levels of stakeholders such as doctors, nurses, administrators, pharmacists and labs. Healthcare Service defines different access control levels to each stakeholder for accessing the healthcare information and we assume Healthcare Service as a trusted entity.

![Mobile Healthcare Architecture](image)

A. Protocol

The protocol addresses the authentication, data integrity, confidentiality and data access control for healthcare information in the mobile healthcare environment. The communication is based on the Simple Object Access Protocol (SOAP) and
the messages are written in the XML format.

\[\text{HO} = \text{Healthcare Operator}\]
\[\text{IdP} = \text{Identity Provider}\]
\[\text{NAF} = \text{Network Application Function}\]
\[\text{Patient} = \text{Patient with a Mobile Device}\]
\[\text{IMPI} = \text{IP Multimedia Private Identity}\]

1) Authentication Phase:
1) The patient requests to access the health services from the HO / IdP attaching his/her IMPI number with the request.
2) If the patient has not been authenticated at this stage, the HO / IdP sends a request to the patient to initiate the Bootstrapping Procedure (BSP).
3) The patient initiates the BSP at the BSF and obtains the B-TID which is a string of base 64 random data and the BSF server domain name. The BSF also generates and sends the key material (Ks) for the secure communication between the HO / IdP and the patient.
4) The patient starts the login procedure by forwarding the B-TID to the HO / IdP.
5) The HO / IdP sends the B-TID to the BSF and obtains the relevant Ks belongs to the B-TID.
6) The HO/ IdP generates a random number and sends that to the patient. The random number is used to challenges the patients ownership to the Ks.
7) Once the patient receives the random number, the Challenge Response is generated and sent to the HO / IdP. The Challenge Response is a function of the random number and the Ks.
8) If the Challenge Response is successful HO / IdP generates and sends the User Token (UT) to the patient, unless it repeats step 6. The content of the UT is encrypted from the Ks.

2) Service Access to Healthcare Service:
1) Once the UT is received, patient can access service providers who are registered under the Healthcare Operator. The patient requests the access to a service provider (SP) from the HO / IdP attaching the SP identity (SPID) and the UT with the request.
2) The patient receives the Service Provider User Token (SPUT) and the temporary session key (tsK) as the response and the response message is encrypted using the Ks. The SPUT is concatenated with SPID, tsK, time stamp (TS) and the patients identification at HO / IdP. This token is digitally signed by the HO / IdP and encrypted using the public key of the SP.
3) The patient sends the SPUT to the SP and initiates the service.
4) If the SPUT is extracted successfully by the SP, it confirms to the patient unless a failure message is sent and the patient should request a new SPUT from the HO / IdP.
5) After obtaining the successful confirmation, patient sends the service request to the SP along with the required data. The data is embedded to the message in the XML format and the message is encrypted using the tsK.

3) Service Access to Healthcare Service: The Healthcare Service (HS) 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. 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 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. The HS generates separate key pairs for each user in the system, saves a copy in the HS and installs it in the user’s application device. It also provides an XML Key Management service to process the key information related with the XML Signature and the XML Encryption.

1) The patient initiates the access with the HS and sends the service request XML. The request message is encrypted using tsK between the HS and the patient. The service request XML is concatenated with the request type, the request receiving party, the patients information and the health information. Let us assume the patient requests a medication from a doctor by sending the health information. So the HS receives the message containing the request type as medication and the receiving party as the doctor. Then the HS identifies that the health information is for the doctor but the patients information should be sent to the healthcare administrator. Since the HS 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 to protect the patients privacy as well as the administrative information should not be visible to the doctor. Therefore the XML element that contains health information in the document is encrypted using the doctors public key and the administrative information is encrypted using the administrators public key. Before the encryption both XML elements are digitally signed by the HS private key for the authentication and finally it is forwarded to the doctor for the medication process.
2) Once doctor receives the XML document, he/she decrypts the XML data elements which are encrypted using his/her public key and verifies the XML signature for the authentication. However the doctor is unable to access the administrative information that is concatenated in the same XML document.
3) Let us assume doctor requires some laboratory results based on the health information. He/she appends a new XML element to the document that includes the health data readings of the patient. The new XML element
should only be extracted by the laboratory. Therefore the doctor signs the XML element for the authentication and encrypts it using the public key of the lab.

4) Once the XML document is received by the lab, it decrypts the XML element using the private key of the lab and verifies the sender from the signature. The laboratory results are embedded to the XML document, signed by the private key of the lab and then encrypted using the doctors public key.

5) The doctor receives the XML document, decrypts the XML data element that was appended by the lab, verifies the labs 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 includes instructions and information to a specific user levels.

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 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 HS public key.

Once all the XML elements are appended successfully the document is forwarded to the nurse.

6) 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. Nurse may include new XML message elements in to the XML document for different users signing each element separately using his/her own private key and encrypted using public keys of the respective receivers. If the message is for the patient then it is encrypted using the HS public key.

7) Once the XML document is received by the pharmacy it decrypts the XML messages that are appended by the doctor and the nurse about medications and also it may append an XML message to the administrator applying the digital signature and also encrypting the message.

8) The XML document is finally received by the administrator of the HS. Administrator extracts the patients information that was appended by the HS and the other XML elements that are encrypted using the administrators public key.

9) Administrator embeds invoicing and other administrative information of the patient into the XML document, signs it using his/her private key and encrypts using the HS public key. Then the XML document is sent to the HS.

10) Once the document is received by the HS it decrypts all the XML messages that are encrypted using its own public key and verifies the senders with XML signatures. These messages contain medication information to the patient; therefore the HS appends all the decrypted XML data elements into the messages, encrypts the complete message using the tsK and sends it to the patient.

11) 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 the XML signature of the sender. Therefore patient can verify signatures using the XML key management feature in the HS.

The same XML document is utilized to send information to the Insurance Providers, Private Medical Centres and other service providers who are interested on the patient’s health situation. The HS appends information required for those parties in to the XML document, signs the information using HS private key and encrypts it using the receiver’s public key. As an example, patient may send the same XML document to the Insurance provider to claim the medical insurance. Insurance provider will only be able to retrieve the invoice data from the document but not the patient’s health information.

IV. CONCLUSION

As the number of ageing population increases there is an increasing pressure on the national and international health care communities to find alternative health care solutions to keep the quality of life of these people at the same levels as before. Due to the increasing usage of mobile handsets by all ages and the functionality and additional features that are available in today’s handsets has made the delivery of health care data possible using the mobile technology. However, as the health care data is sensitive it has to be protected against hackers and intruders. In this paper the authors have shown that by using the XML cryptographic technologies and role based authorization the electronic patient data can be secure and protected against the malicious users.

REFERENCES


APPENDIX

XML Data to be encrypted

<?xml version="1.0" encoding="utf-8"?>
<HealthInfo>
  <Name>Ian Daneal</Name>
  <Bloodpressure>132</Bloodpressure>
</HealthInfo>
Encrypted XML Data

<?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>

<?xml version="1.0" encoding="utf-8"?>
<HealthInfo>
  <Name>Ian Denley</Name>
  <Bloodpressure id="bloodpressureReading">132</Bloodpressure>
  <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">
        <Transform
          Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>j6lwx3rvXFO0vXKtMup4NbeVu8nk=</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>
</HealthInfo>