Trust Delegation for Medical Records Access using Public Mobile Networks

Dasun Weerasinghe, Muttukrishnan Rajarajan and Veselin Rakocevic
School of Engineering and Mathematical Sciences
City University London.
dasun.weerasinghe@city.ac.uk

Abstract—**This paper provides detailed solutions for trust delegation and secure temporary storage of medical records for authorized users in public mobile communication networks. The solutions presented in this paper enable the development of software that can be used by emergency medical units in urgent need of sensitive personal information about unconscious patients. In today's world, technical improvements in mobile communication systems mean that users can expect to have access to data at any time regardless of their location. While this paradigm is a natural goal for both service providers and users in commercial applications, for the exchange of sensitive personal medical information authentication and security present major challenges. This paper presents a token-based procedure for the delegation of trust between a requesting mobile unit and secure medical data storage. Once the trust is established, the received data should only temporarily be available. Our paper presents the design of the proposed solutions and gives details of the software demonstration developed in our research group.**

I. Introduction

In the modern world people are getting used to having access to a wide range of data and applications wherever they are and whenever they want, using public mobile communication networks. In such a ubiquitous communication environment, it is not a surprise that there is a growing need to enable the emergency medical teams to have a continuous and secure access to patient medical records. The added benefit of having person's medical record while providing emergency care is obvious, and has been highlighted in a number of publications [3][18][16][6][17].

This paper provides a detailed analysis of the above issues and provides solutions for secure authentication of data download and data protection following the download. In this respect, the first issue that requires attention is the secure authentication. This is achieved by careful distribution of trust between the key players in the process: the medical provider storing the medical records, the mobile network, and the mobile device requesting the data. Trust had to be negotiated and delegated between these players to enable them to feel confident to exchange data. Trust negotiation is an approach to access control on sensitive attributes, whereby access is granted based on the trust established between the service requester and the service provider [20]. The traditional approaches to establishing trust include either minimizing the security protection of the data (e.g. without using credentials for authorization) or considering that the parties are not strangers and present access to obtain services [28]. It is usually assumed that the trust negotiation process should be ubiquitous - available anytime, anywhere, independent of software layers, independent of platforms, wherever strangers might wish to interact, using fixed or mobile devices. However, with the rapid growth of security vulnerabilities and increased sensitiveness of the data, there is a need for novel, secure trust negotiation protocols.

With the emergence of electronic health solutions, the delegation and negotiation of trust from one healthcare service provider (HSP) to another is one of the main requirements for the secure provision of data and services [21][12]. The healthcare service providers can "in the extreme case" be mutually unknown and therefore not trusting each other. In our paper, the HSPs are classified in two categories; the 'relying healthcare service provider' and the 'requesting healthcare service provider'. The relying HSP is a medical center or a hospital which stores sensitive patient medical records - including patient's medical history, current diagnosis and medical treatments, known allergies, social history of the patient and patient personal information. The patients have the ownership of the patient medical records but they have granted the trust delegation on accessing these records to their HSP [19]. The requesting HSP is another medical center, hospital or mobile healthcare service unit with doctors and/or paramedics. This HSP requests access to patient medical records from the relying HSP in order to perform special or urgent diagnosis and medical treatment to patients. The access to the patient medical record is vital for a doctor at the requesting HSP to perform a correct diagnosis and/or treatment.

In order to gain access to the data, the requestor HSP has to obtain the trust of the relying HSP. Crucially, the process of trust negotiation needs to be simple and compatible with the operation of the mobile network and the mobile service application on the mobile devices in use at the requestor HSP.

To understand fully the application of secure solution presented in this paper, assume that a person, previously registered with his town medical center where his medical record is stored, has a traffic accident and is unconscious, being treated by an emergency medical team. The emergency team immediately request access to the patient medical record, to facilitate the correct treatment. In this way a member of the emergency healthcare team becomes the requesting HSP and makes a request (on behalf of the team) to the relying HSP - the patient's medical center. The two HSPs then use the public mobile network to exchange special tokens to negotiate

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6057
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6057

the trust between each other. Once this is done, the trust is delegated to the emergency team and they have access to the patient medical record.

This paper provides a detailed solution for securing the above scenario. The analysis presented in the paper focuses on the provision of security in the Web Services environment. The Web Services (WS) is the latest Internet standard specifying the interoperability, security and accessibility issues for the distributed Internet applications. Applications of WS security solutions in public mobile networks are very rare. The paper is organized as follows. Section 2 presents the related work and requirement on trust negotiation and mobile services for healthcare. The proposed architecture and system design principles are discussed in Section 3 and Section 4.

II. Trust Negotiation in Mobile Services

During the recent past, initiatives have been taken both by the academia and by the industries towards improving the use of mobile communication for healthcare and safety of the public [14]. The m-health is an existing term representing an emerging set of healthcare applications and services that people can access from their web-enabled mobile devices [10]. Medical personnel having access to clinical data irrespective of the geographic location is an advantage of m-health. There are numerous examples of interesting applications. For example, real-time mobile telemedicine system is introduced to transmit video and patient bio-signals from a moving ambulance to a doctor in the hospital using wireless cellular phones [27]. Mobile device in the ambulance is connected to a Web service in the hospital to retrieve advices about transferring the patient there [15]. These approaches allow medical personnel to access patient medical records from a remote location but only if the patient medical records are at a centralized or distributed location for public access. Generally patient medical records are stored at patient's medical center and access to those records are restricted to protect the data confidentiality and patient privacy. Therefore mobile medical personnel at the disaster scene has to prove the legitimacy to access patient medical records from the patient's medical center [19].

The process on proving legitimacy and allowing access to patient medical records is known as trust negotiation. The research on trust negotiation between entities has been carried out by a number of research groups and these groups proposed a number of trust negotiation and evaluation algorithms based on the trust negotiation concepts [5].

Automated trust negotiation can be defined as a process of establishing trust between mutually unknown parties through the exchange of digital credentials [24]. These credentials contain private sensitive information [23] and those have to be exchanged through a trusted entity or a trusted media. The trusted entity can be an administrative body of the network and should be able to authenticate trust negotiating parties. The trust negotiation and interaction among strangers may often occur with no proper knowledge of each other [9]. A trust relationship framework for healthcare information system, based on performing sensitive transactions via the mutual disclosure of attributes contained within digital credentials is presented in [21]. In [20], Trust-Serv is a model driven trust negotiation framework for Web services, which features a policy language based on state machine. Winslett M. et al [24] have proposed a TrustBuilder framework which can support automated trust negotiation between strangers on the Internet. This proposal suggested privacy protection and trust negotiation in Single-Sign-On environment as future research direction. Finally, authors of [2] present dynamic trust negotiation approach that supports for decentralized access control over organizational boundaries for e-health information. This is an online solution to interact between different healthcare portals.

A trust negotiation process should incorporate a trust negation algorithm to identify, verify and validate the trust level of the requestor party with respect to the requesting information. There are number of trust negotiation algorithms available and our framework will be able to use any of those to generate the trust level between the requestor party and relying party. Wu Z. et al describes an indirect trust establishment mechanism to bridge and build new trust relationships from extant trust relationships [26]. Meanwhile he has presented another trust negotiation framework based on Web services and Token exchange for electronic business domain [25]. Trust tickets and session tickets are discussed by Bhargav-Spantzel A. et al [4] and these are used to identify the sufficiency of the trust level before disclosing sensitive resources. The paper [5] introduces fuzzy logic into the definition and evaluation of trust in a federated trust management. Fuzzy logic can help to handle uncertainty caused by indirect information and subjective judgment in trust management. The trust evaluation algorithms output a trust level defined in the rage of Full to Minimal such as Full, High, Medium, Low, Minimal or the rage is in numerical numbers such as 1 to 10 [11].

Transferring trust delegation for accessing patient medical records between healthcare service providers is one of the vital requirements in healthcare industry and specially accessing patient medical records over a mobile device in emergency situations. According to the knowledge of authors most publications haven't considered the security and privacy aspects in trust negotiation techniques for mobile healthcare environment. Therefore the novelty and the research contribution of this paper compared to the other publications is; 'Token based trust negotiation and delegation framework for healthcare service providers. This trust negotiation framework is protected from security vulnerabilities and it is based on Mobile Web services architecture'.

III. Architecture

Our architecture consists of five main actors: Trust Granting Server (TGS), relying healthcare service provider, requesting healthcare service provider, mobile healthcare personnel from requesting healthcare service provider and patient, as shown in Figure 1. The mobile healthcare personnel has a bandwidth constrained mobile device connected to a mobile operator network. The patient is registered with the relying healthcare service provider.

The relying healthcare service provider maintains patient medical records in data storage and it has a mobile Web

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6057
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6057

services interface to handle service requests over the Internet. As shown in Figure 1, the MHP is at the disaster situation with the patient, and the MHP requires the patient medical records from the relying healthcare service provider. The patient medical records will be downloaded to the mobile device through the mobile Web services interface over the Hypertext Transfer Protocol (HTTP). However, the requestor healthcare service provider and the MHP have to negotiate the trust with the relying healthcare service provider before the disclosure of the patient medical records. The trust negotiation process is administrated and maintained by the TGS. The TGS acts as an identity provider and trust negotiator between the healthcare service providers. Therefore the TGS has to maintain identification and authentication details of each healthcare service provider. The authentication and trust negotiation services at TGS are implemented based on the Service Oriented Architecture (SOA) and it provides an application programming interface (API) for healthcare service providers to connect and execute service methods. The TGS should be a trusted entity among healthcare service providers and patients. Therefore the National Health Service (NHS) in the UK, the U.S. Department of Health & Human Services (HHS) in the USA, Medicare in Australia, mobile operators such as T-Mobile, Vodafone and government based organization are some of the potential candidates for the trust granting role.

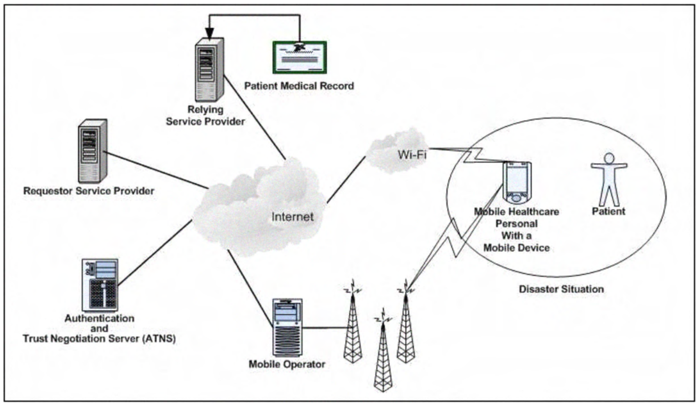

Fig. 1. Proposed Architecture

IV. Proposed Schema

The solution for trust negotiation in mobile web services is designed using the token based trust negotiation framework. The TGS is the facilitator for the trust negotiation between healthcare service providers. It generates and issues tokens for authentication and trust negotiation process. These tokens are designed in XML format and those are categorized into security tokens and trust tokens. The mobile device is unlikely to be trusted by the schema but the security capsule is a trusted entity. So patient medical records and obtained tokens are stored in the security capsule. The patient medical records are stored in the encrypted format and security capsule can decrypt those only if valid security and trust tokens are present.

The use case for trust delegation on patient medical records begins when MHP attempts to access patient medical record from a healthcare service provider. The patient medical records are saved at the relying healthcare service provider and TGS bridges the trust negotiation between two parties. The scheme for transferring trust delegation to access patient medical records is summarized with the reference to Figure 2.

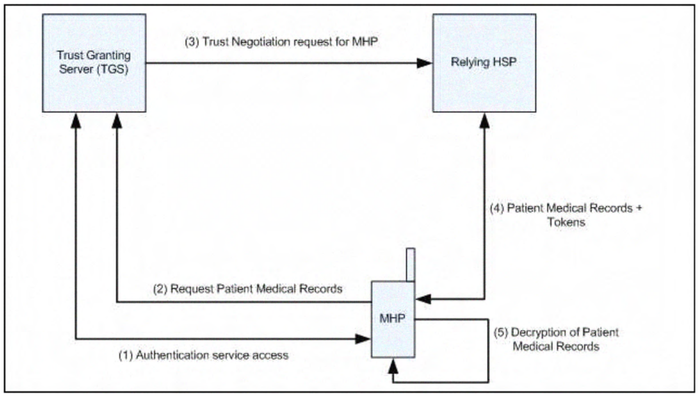
Trust Granting
Server (TGS)
(3) Trust Negotiation request for MHP
Relying HSP
(4) Patient Medical Records +
Tokens
(2) Request Patient Medical Records
MHP
(5) Decryption of Patient
Medical Records
(1) Authentication service access

Fig. 2. Scheme Description

1) The MHP authenticates with TGS to access patient medical records. The TGS issues the security token to the MHP's mobile device
2) The MHP requests the access to patient medical record from TGS by specifying the patient identity
3) The TGS locates the relying healthcare service provider for the patient medical records and sends the trust negotiation request
4) The patient medical record and trust tokens are sent to the mobile device of MHP from the patient's healthcare service provider
5) The mobile device decrypts the patient medical records utilizing the tokens records.

A. Trust Granting Server model

The trust negotiation is one of the main tasks of the TGS. It initiates the trust negotiation process by evaluating the trust level of the MHP against the relying healthcare service provider. The MHP is introduced to the relying healthcare services with the derived trust value. The trust value is derived using the trust evaluation engine. The previous trust negotiation records of the MHP are saved in the Trust mapping database and those will be utilized to generate an effective trust value for the MHP. The trust mapping database maintains information about trust establishment and trust rejection decisions between users and service providers with the date and time of the instance.

The generation of the trust value is executed at the Trust Evaluation Engine and it can be implemented using some of the trust negotiation algorithms and models [4][7][25][26]. The performance and the implementation of this trust evaluation algorithm is beyond the scope of this publication. The model of the TGS is shown in the Figure 3. The Web services interface establishes communication with 3rd parties and the business logic is implemented in the TGS engine.

V. Implementation

Web Services are defined as software systems that support interoperable network interactions. In particular Mobile Web

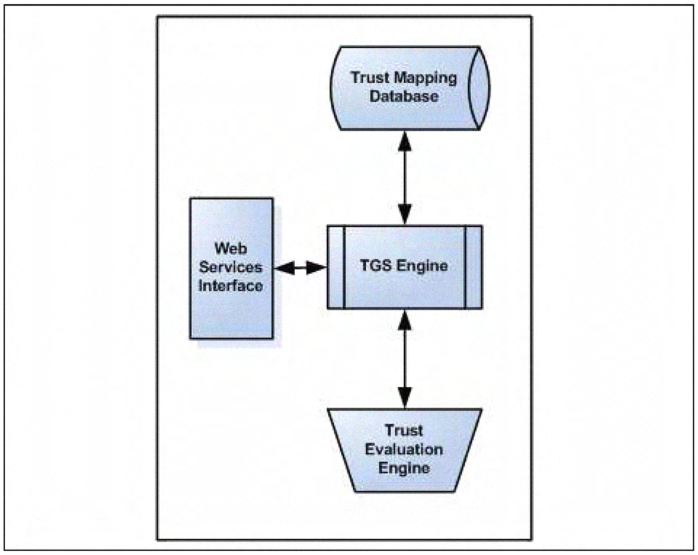

Fig. 3. Trust Granting Server model

Services is a comprehensive, up-to-date and practical guide to adapt mobile Web services-based applications [8]. They allow implementation of a service-orientated architecture incorporating services at the host. All the services are available on SOAP protocol and those are structured as XML messages. The authors have considered these constrains during the implementation including the bandwidth constrains for message communication. The paper presents both specific protocol exchanges and the structure and syntax of security and trust tokens.

A. Prerequisites for protocol

The protocol uses both symmetric and asymmetric cryptographic techniques to provide the authentication, confidentiality and integrity services. The following requirements must be met prior to the use of the protocol:

- All actors have agreed on a specific signature algorithm for data integrity
- All actors have agreed on an asymmetric encryption algorithm for data confidentiality
- All actors must have encryption key pair for encryption scheme, and all the actors possess a trusted copy of the public key for the other actors
- All actors must have integrity key pair for signature scheme, and all the actors possess a trusted copy of the public key for the other actors
- The login token is generated by the relying healthcare service provider of the MHP and it is stored in the mobile device.
- Healthcare service providers are register with the TGS. Meanwhile each MHP is uniquely identified at TGS and the identity is resided in the mobile device.

B. Protocol

This section describes the critical protocol exchanges to address the threat model with the consideration of authentication, confidentiality and integrity. The protocol consists of 3 phases:

1) MHP authenticates with TGS
2) Trust negotiation between relying healthcare service provider and MHP
3) Disclosure of patient medical records to the MHP

The following additional notations are adapted for the protocol explanation:

- RelHSP= Relying healthcare service provider
- ReqHSP= Requesting healthcare service provider

*1) **Phase 1: MHP authenticates with the TGS** :*

Phase 1 initiates with MHP going to a disaster scene. The mobile device of MHP had the Login Token that was generated by the healthcare service provider.

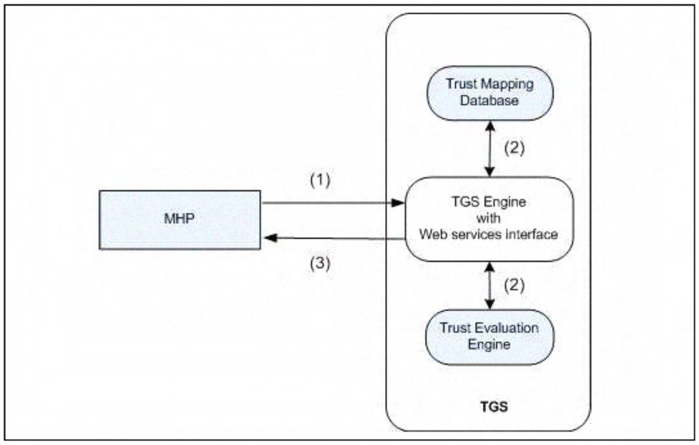

Fig. 4. Phase 1 message flow

Following are the steps to get the MHP authenticated with the TGS:

1) MHP to TGS [Login Token]; The login token is the authentication request to the TGS from MHP. The token consists of information about the healthcare service provider and mobile healthcare personal. The login token is signed by the private key of ReqHSP for the token integrity. The security capsule encrypts the token with the TGS public key to protect the message confidentiality.
2) The TGS decrypts the message using its private key and verifies the signature of the token against the public key certificate of ReqHSP. If the verification is successful then the ReqHSP and MHP identification are checked in the Trust Mapping Database.
3) TGS to MHP [Authentication Token]; Once the trust level is obtained, the TGS generates the Authentication Token for MHP. This authentication token represents MHP's authentication to access TGS services. The authentication token is sent to the MHP over the secure channel using the Public Key Infrastructure (PKI) of MHP. The token consists of MHP identity, ReqHSP identity, MHP trust level, time stamp and token life time. It is encrypted and signed by confidentiality and integrity keys of TGS.

*2) **Phase 2: Trust Negotiation between MHP and Relying Healthcare Service provider** :*

Phase 2 startes with MHP approaching a patient at a disaster situation. The patient needs urgent medical attention and

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6057
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6057

MHP has to view the patient medical records for effective treatments. It is assumed that MHP has found an identification of the patient. The TGS uses this identification to identify the patient and the healthcare service provider of the patient. The source of identification is defined by the TGS and the possible approaches are; an Identification issued by the TGS, SIM based identification from patient's mobile device [22], application based identification from patient's mobile device, full name with date of birth or patient's finger print.

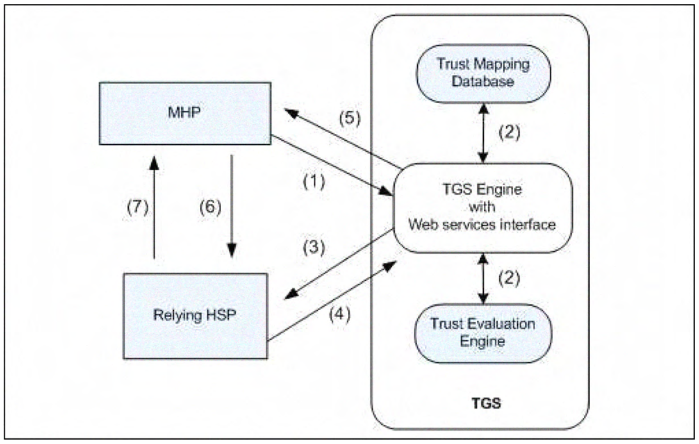

Fig. 5. Phase 2 message flow

Following are the steps on trust negotiation between the healthcare service provider and the MHP:

1) MHP to TGS: [RecordAccess(PatientID, Authentication Token)]; The MHP identifies the patient and makes the request to access patient medical records.
2) The TGS verifies the authentication token and then identifies the relying healthcare service provider (RelHSP) of the patient. The RelHSP holds the patient medical records. Then TGS locates the previous trust negotiation and trust decline records between the requesting parties (MHP and ReqHSP) and the relying party (RelHSP) in the trust mapping database. The Trust Evaluation Engine generates the recommended trust level for MHP to access patient medical records from RelHSP.
3) TGS to RelHSP [TrustRecommendation Token]; The Trust Recommendation Token is generated by the TGS and it consists of MHP identification, ReqHSP identification, MHP profile information, recommended trust level for MHP, MHP public key certificate and patient identification. The Trust Recommendation Token is encrypted using the public key of the RelHSP and it is signed using the private key of TGS.
4) RelHSP to TGS [TrustChallenge, Confirmation, Assigned Trust Level]; The RelHSP verifies the Trust Recommendation Token against the TGS signature and obtains the information about the requesting party and patient identification. The RelHSp can either re-evaluate the trust level of the MHP using one of the trust evaluation algorithms [4][7][25][26] or it accepts the trust level recommended by TGS. The finalized trust level for MHP is named as 'Assigned Trust Level' and then the trust challenge token is generated by RelHSP. The Trust Challenge token consists of Random number (RAND), RelHSP public key certificate, patient identification, RelHP identification and MHP identification. The Trust Challenge token is signed by the private key of the RelHSP and it is encrypted by the public key of MHP. Meanwhile the RelHSP informs the assigned trust level to TGS and this information is updated to the trust mapping database.
5) TGS to MHP [TrustChallenge Token]. The TGS sends the Trust Challenge Token to the MHP.
6) MHP to RelHSP [TrustChallengeResponse]. The MHP retrieves the RAND from the trust challenge token and generates the trust challenge response using its private key for integrity. The Trust Challenge Response is encrypted using the public key of RelHSP to protect the confidentiality.
7) RelHSP to MHP [Trust Token]. The RelHSP validates the trust challenge response against the RAND and public key certificate of MHP. If the validation is successful then the Trust Token is generated as trust delegation object. The Trust Token consists of session key, time stamp, token lifetime, RelHSP identification, MHP identification, patient identification and assigned trust level. Token is signed with the private key of the RelHSP and encrypted with the public key of the MHP.

*3) **Phase 3: Patient Medical records are shared with MHP:***

The trust token which is the trust delegated object for accessing the patient medical record is saved in the security capsule. Patient medical records (PMR) are sent in encrypted format from RelHSP to MHP.

1) RelHSP to MHP [Encrypted Patient Medical Record]. The patient medical records are encrypted using the session key of the Trust Token. Then it is signed by the RelHSP private key for integrity and encrypted by the MHP public key for confidentiality.
2) The mobile device of MHP obtains the encrypted patient medical record data and it decrypts the data using the session key in the trust token. If the lifetime of the Trust Token is expired then the MHP requests a new Trust Token by sending the expired Trust Token to RelHSP.

C. Token Generation and Management

The trust negotiation and delegation depends on the token exchange and token verification. The mobile healthcare personnel gets access to patient medical records only if valid tokens are present in the security capsule. Therefore the security capsule maintains a special storage area for token storage. The authors have taken careful design considerations to reduce the complexity and size of these tokens. Meanwhile the proposed protocol is optimized to minimum number of communication messages in the authentication and trust negotiation processes [22][13]. Therefore the proposed schema is suitable for processing power and capacity constrained mobile devices in the bandwidth constrained mobile networks. This section describes the token structures for the proposed schemas and the below abbreviations are used for token representation.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6057
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6057

$$\begin{aligned} [Y]ID &= \text{Unique identification of Y in the system} \\ TS &= \text{Time stamp} \\ tsK &= \text{Session Key} \\ s_{N_K}(\text{X}) &= \text{The signature of data X using secret key K of N} \\ e_{N_K}(\text{X}) &= \text{The encryption of data X using secret key K of N} \end{aligned}$$

- Login Token (LT)
  (LT = $s_{ReqHSP_{private}}$[ReqHSPID | MHPID | MHP Profile]);
  The Login Token is generated by the healthcare service provider of the mobile personnel and it is stored in the mobile device. The MHP uses the Login Token as authentication credentials to access TGS services. The MHP profile contains the mobile healthcare personal information including the access level privileges.

- Authentication Token (AT)
  (AT = $e_{TGS_{S1}}(s_{TGS_{S2}}$[ReqHSPID | MHPID | GTL | Token Life Time | TS]));
  The Authentication Token is issues by the TGS for authenticated mobile healthcare personals. This token is belonged to the TGS and this can only be viewed and verified by the TGS. Therefore the token is signed by TGS integrity key (TGS2) and then encrypted by the confidentiality key of TGS (TGS1). This token specifies the General Trust Level (GTL) of the MHP. This trust level is derived using the trust negotiation algorithm at TGS. The timestamp and token life time are included to verify the token freshness.

- Trust Recommended Token (TRT)
  (TRT = $e_{RelHSP_{public}}(s_{TGS_{private}}$[ReqSPID | MHPID | RTL | MHP Profile | PatientID | TS | MHP PKI Cert]));
  The Trust Recommended token is used by TGS to negotiate the trust between the mobile healthcare personnel and the patient's healthcare service provider (RelHSP). The TRT is generated by the TGS and it is encrypted with the public key of the relying healthcare service provider for confidentiality and the integrity is protected by signature of token with TGS private key. The TGS inserts the recommended trust level (RTL), the MHP profile information and Patient identification into the token. This information will be assists at healthcare service provider domain to make the trust delegation decision. The RTL is generated by the TGS against the previous trust negotiation records between the two parties. The public key certificate of the MHP is inserted for establishment of secure communication link between the RelHSP and MHP for future commutations. Timestamp (TS) will be used to verify the message freshness at the RelHSP.

- Trust Token(TT)
  (TT = $e_{MHP_{public}}(s_{RelHSP_{private}}$[TTID | MHPID | ATL | PatientID | Token Life Time | TS | tsK]));
  The trust token is the trust granted object for MHP to access the requested patient medical record. The trust token identification (TTID) is assigned to each trust token for unique identification. The relying service provider inserted the finalize trust level for the MHP which is named as assigned trust level (ATL). The trust token is linked with a patient medical record and therefore the patient identification is inserted into the token. The Trust Token is signed by the private key of the relying healthcare service provider and the confidentiality is protected by encrypting the token using the public key of MHP. The tsK is the session key is used to decrypt the encrypted patient medical records. Once the trust token is expired the MHP has to request a new trust token from the issuer of the token. The timestamp (TS) and token life time are used to verify the token freshness before the utilizing it.

D. *Proof of concept prototype*

A proof of concept system is developed by the authors to validate the proposal in this paper.

The business logic of TGS, relying service provider and requesting service provider are implemented in J2EE environment and then those are deployed in Axis 2.0 Web services engine. Axis 2.0 is a SOAP processor that has been developed as an Apache open source project. The business logic implementation connects with MySQL database for storing user access details, patient medical records and trust negotiation records. The Axis 2.0 web service engine is deployed on top of the Apache Jakarta Tomcat 6.0 server. This will enable service methods in the web service interface to invoke over HTTP messages. Latest JDK environment should be installed in the system before the Tomcat 6.0 installation.

Communication between Web Services as well as Web Services and Mobile client has been developed using SOAP messages over HTTP. Axis client is also included in some of the Web Services to invoke services in another Web service. The extra Web services security is enabled for Web services communications with Ws-Security functionalities. Web Services Definition Language (WSDL) document for each web service is created by the Axis 2.0 Engine and this document is used to publish the service methods available to invoke.

According to the protocol communication between all the entities are secured using java.security and javax.crypto libraries. All tokens and sensitive attributes are signed and encrypted before appending to the SOAP message. VeriSign's Trust Services Integration Kit is used to generate XML signatures.

The demonstration environment of our proof of concept model is implemented in J2ME and J2EE. J2ME provides the necessary implementation for Mobile device simulation and J2EE provides the web service implementation and deployment. This model is designed to verify the trust negotiation between two healthcare service providers and trust delegation of patient medical records to a mobile user for a limited time period in a secure environment with protecting the patient privacy.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6057
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6057

VI. Conclusion

The paper has introduced a scheme for the trust negotiation between healthcare service providers to retrieve and access patient medical records using mobile devices during an emergency scene. The Liberty Alliance Single Sign On models is extended to design the authentication and trust negotiation processes of the scheme. The main contribution of the paper can be summarized as; 'Trust negotiation and delegation framework for mobile healthcare'. The contribution of system architecture, scheme and protocol will form a new business model for healthcare industry to efficiently and quickly share data and services between unknown healthcare service providers. This approach will improve healthcare service facilities and finally it will improve the quality of life of citizens.

References

[1] Java technology for the wireless industry (jsr 185). June 2003. Java 2 Platform, Micro Edition, Sun Microsystems.

[2] Oluwafemi Ajayi, Richard Sinnott, and Anthony Stell. Dynamic trust negotiation for flexible e-health collaborations. In *MG '08: Proceedings of the 15th ACM Mardi Gras conference*, pages 1–7. ACM, 2008.

[3] M.A. Belsis and Dwivedi A.N. Providing secure maccess to medical information. *Int. J. Electronic Healthcare*, 3(1):51–57, 2007.

[4] Abhilasha Bhargav-Spantzel, Anna C. Squicciarini, and Elisa Bertino. Establishing and protecting digital identity in federation systems. *J. Comput. Secur.*, 14(3):269–300, 2006.

[5] N Borselius. Mobile agent security. volume 14, pages 211–218, Oct. 2002.

[6] Sam Campbell, Gordon L. Gibby, and Susan Collingwood. The internet and electronic transmission of medical records. *Journal of Clinical Monitoring and Computing*, 13(5):325–334, Sep. 1997.

[7] D. Dean, Felten, and Wallach. Java security: From hotjava to netscape and beyond. In *SP '96: Proceedings of the 1996 IEEE Symposium on Security and Privacy*, page 190, Washington, DC, USA, 1996.

[8] Hirsch F., Kemp J., and Ilkka J. Mobile web services: Architecture and implementation. J. Wiley & Sons.

[9] Adam Hess, Jason Holt, Jared Jacobson, and Kent E. Seamons. Content-triggered trust negotiation. *ACM Trans. Inf. Syst. Secur.*, 7(3):428–456, 2004.

[10] R.S.H. Istepanian, E. Jovanov, and Y.T. Zhang. Guest editorial introduction to the special section on m-health: Beyond seamless mobility and global wireless health-care connectivity. *Information Technology in Biomedicine, IEEE Transactions on*, 8(4):405–414, Dec. 2004.

[11] D. I. Jung and B. J. Avolio. Opening the black box: an experimental investigation of the mediating effects of trust and value congruence on transformational and transactional leadership. *Journal of Organizational Behavior*, 21(8):949–964, DEC. 2000.

[12] Robert K. Knopp and Paul A. Satterlee. Confidentiality in the emergency department. *Emergency Medicine Clinics of North America*, 17(2):385–396, May 2005.

[13] John A. MacDonald, William G. Sirett, and Chris J. Mitchell. Overcoming channel bandwidth constraints in secure SIM applications. In *Security and Privacy in the Age of Ubiquitous Computing*, pages 539–549. Springer Science and Business Media, 2005.

[14] E.B. Moran, M. Tentori, V.M. Gonzalez, J. Favela, and A.I. Martinez-Garcia. Mobility in hospital work: towards a pervasive computing hospital environment. *International Journal of Electronic Healthcare*, 3(1):72–89, 2007.

[15] Enrico Motta, John Domingue, Liliana Cabral, and Mauro Gaspari. Irs-ii: A framework and infrastructure for semantic web services. In *2nd International Semantic Web Conference (ISWC2003)*, pages 306–318. Springer-Verlag, 2003.

[16] Miguel A. Mu, Marcela Rodrguez, Jesus Favela, Ana I. Martinez-Garcia, and Victor M. Gonzlez. Context-aware mobile communication in hospitals. *Computer*, 36(9):38–46, 2003.

[17] David M. Rind, Isaac S. Kohane, Peter Szolovits, Charles Safran, Henry C. Chueh, and G. Octo Barnett. Maintaining the confidentiality of medical records shared over the internet and the world wide web. *Ann Intern Med*, 127(2):138–141, 1997.

[18] M.D. Rodriguez, J. Favela, E.A. Martinez, and M.A. Munoz. Location-aware access to hospital information and services. *IEEE Transactions on Information Technology in Biomedicine*, 8(4):448–455, Dec. 2004.

[19] R. Schoenberg and C. Safran. Internet based repository of medical records that retains patient confidentiality. *British Med. J.*, 321:1199–1203, 2000.

[20] Halvard Skogsrud, Boualem Benatallah, and Fabio Casati. Model-driven trust negotiation for web services. *IEEE Internet Computing*, 7(6):45–52, 2003.

[21] David K. Vawdrey, Tore L. Sundelin, Kent E. Seamons, and Charles D. Knutson. Trust negotiation for authentication and authorization in healthcare information systems. In *Proceedings of the 25th Annual International Conference of the IEEE*, Sep. 2003.

[22] Dasun Weerasinghe, Kalid Elmufti, Muttukrishnan Rajarajan, and Veselin Rakocevic. Securing electronic health records with novel mobile encryption schemes. *International Journal of Electronic Healthcare*, 3(4):395–416, 2007.

[23] William H. Winsborough, Kent E. Seamons, and Vicki E. Jones. Automated trust negotiation. *DARPA Information Survivability Conference and Exposition,*, 1:0088, 2000.

[24] Marianne Winslett, Ting Yu, Kent E. Seamons, Adam Hess, Jared Jacobson, Ryan Jarvis, Bryan Smith, and Lina Yu. Negotiating trust on the web. *IEEE Internet Computing*, 6(6):30–37, 2002.

[25] Zhengping Wu and Alfred C. Weaver. Dynamic trust establishment with privacy protection for web services. *IEEE International Conference on Web Services*, 0:811–812, 2005.

[26] Zhengping Wu and Alfred C. Weaver. Bridging trust relationships with web service enhancements. In *ICWS '06: Proceedings of the IEEE International Conference on Web Services*, pages 163–169, 2006.

[27] Yan Xiao, David Gagliano, Marian LaMonte, Peter Hu, Wade Gaasch, Ruwani Gunawadane, and Colin Mackenzie. Design and evaluation of a real-time mobile telemedicine system for ambulance transport. *J. High Speed Netw.*, 9(1):47–56, 2000.

[28] Ting Yu and Marianne Winslett. A unified scheme for resource protection in automated trust negotiation. In *SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy*, page 110, 2003.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6057
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6057