32nd Annual International Conference of the IEEE EMBS
Buenos Aires, Argentina, August 31 - September 4, 2010

Custom HL7 V3 Message Provider using Web Services Security Features

Javier Voos, Guillermo Riva, Carlos Zerbini, Carlos Centeno and Eduardo Gonzalez

Abstract— **Due the availability of new data transmission technologies and new standards for medical studies development, e-health systems have had a sustained adoption in recent years. In this scenario, the health systems are incorporating and increasing the health services offering in response to their needs. This paper presents a system able to transmit medical studies using different communication channels providing an effective use of the medical equipment, the data transmission networks and the human resources availability. This system is based on service oriented architecture (SOA) to propose different alternatives in terms of which data needs to be transmitted for the acquired medical study, in order to attend different medical diagnosis providing an efficient use of the available communication channels.**

About the security implemented for the data transmission, there are different configurations available for encryption and signing at message level, to ensure that messages cannot be changed without detection during the transmission. For message definition, the HL7 V3 standard is implemented and the medical studies are stored in a centralized database located in a web server accessible via Internet to enable second medical opinion from other specialists.

I. Introduction

THE healthcare standards adoption enables interoperability between e-health systems allowing medical studies processing from external systems or acquired by medical devices from different manufacturers. One of the issues for a standard adoption is related to the increase of the data size needed to save or transmit one medical study, because the system providers have to represent the acquired medical data following the data models defined by the selected standard. In the case of HL7 V3 [1], the requirement to support the reference information model (RIM) for the entities participating in one medical study and the XML [2] tags used for data representation implies the need of high bandwidth for the reachable communication channel in order to allow HL7 V3 well formed messages transmission. Therefore, many e-health systems are using proprietary formats to represent medical data in order to have a limited message size. Aligned with this, only basic security at transport level is guaranteed through the Secure Socket Layer (SSL) protocol, because the implementation of security at message level involves further increasing the message data size with the security-related content.

Manuscript received March 30, 2010.
Javier Voos is with the Clinical Engineering R&D Center (e-mail: jvoos@scdt.frc.utn.edu.ar).
Guillermo Riva is with the Clinical Engineering R&D Center (e-mail: griva@scdt.frc.utn.edu.ar).
Carlos Zerbini is with the Clinical Engineering R&D Center (e-mail: czerbini@electronica.frc.utn.edu.ar)
Carlos Centeno is with the Clinical Engineering R&D Center (e-mail: ccenteno@scdt.frc.utn.edu.ar)
Eduardo Gonzalez is with the Clinical Engineering R&D Center (e-mail: egonzalez@scdt.frc.utn.edu.ar)
Universidad Tecnológica Nacional, Facultad Regional Córdoba, Córdoba, Argentina. Phone: +54 351-598-6001 ext 1136. Fax: +54 351-468-1823.

II. Methodology

To enable the HL7 V3 messages transmission using message level security, a system based on service oriented architecture (SOA) was developed with the following purposes:

1.- To offer configuration parameters to enable partial medical study transmission that meets a specific medical diagnosis.
2.- To adopt HL7 V3 reference information models in order to facilitate transmission, interchange and store of medical studies.
3.- To implement message level security through the WS-Security standard [3] offering encryption and digital signature as alternatives.

A. Architecture

Regarding the software design phase, a service oriented architecture (SOA) was selected analyzing factors like the reuse of existing software components implemented in other projects [4], runtime environment and adaptability for the different security and messaging configurations needed.

At the beginning, after a service identification and scope definition phase, one candidate services list was defined to meet all the features defined as system requirements. The candidate services list was later refined, composing and decomposing services in order to satisfy the same needs in different system modules along the architecture. Having the definitive services list; software components, data model and communication interfaces were developed for their implementation.

Fig. 1 shows the architecture diagram containing these layers:

Operational Systems: external software applications supporting the system. It includes the keystores for security certificates, the libraries running on the medical equipment and the HL7 related applications.

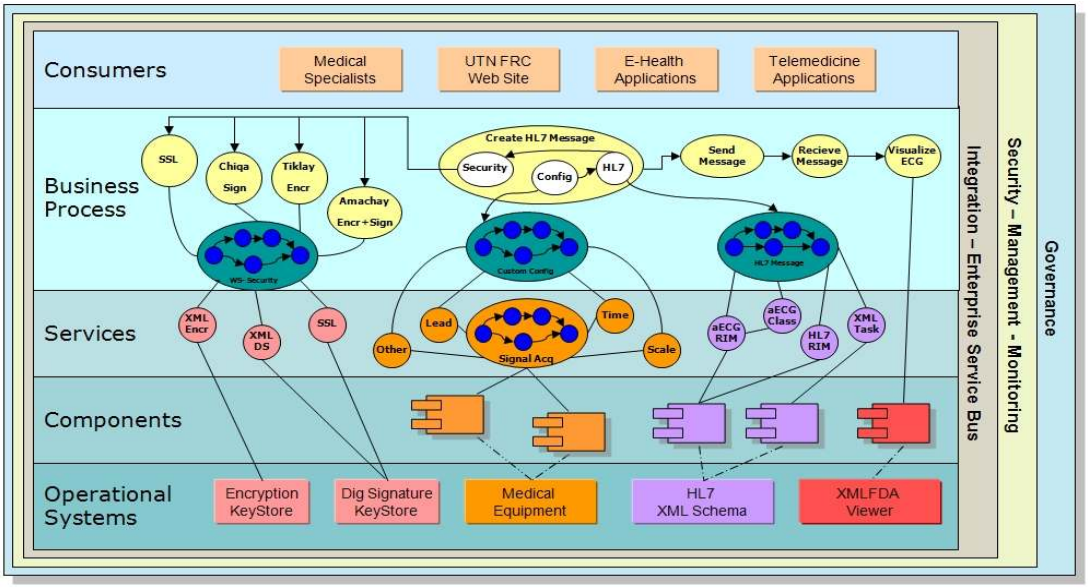

Fig. 1. Service oriented architecture (SOA) diagram for HL7 V3 messages transmission

Components: developed software modules in order to implement the services operations.

Services: specification of software functions available from the components and operation systems layers. This specification provides sufficient detail to invoke the functions exposed in a platform-independent manner.

Business Process: covers the process representation, and building blocks for composing services as a sequence process.

Consumers: provides the capabilities required to deliver HL7 messages to the medical specialists. This layer includes the interfaces for e-health/telemedicine applications communication.

There are also horizontal layers (*Governance*, *Security*, *Integration*, etc) that relate to the overall functionality of the SOA solution. These features are provided by vendor product capabilities running in the IT operating environment.

The business process -*Create HL7 Message*- responsible for the HL7 message creation is implemented by three activities referenced in the architecture diagram (Fig. 1) with the following names: *Security*, *Config* and *HL7*. The *Config* activity implements the services for processing only the medical study section needed in response to the input parameters managed by the *Custom Config* service. The *HL7* activity is represented by a services domain which implements the HL7 V3 reference information models, including functions like message construction/validation, XML processing and application objects model mapping.

Finally, the *Security* activity provides the security at message level implementing the WS-Security standard offering three configurations: signing (Chiqa), encryption (Tiklay) and signing + encryption (Amachay).

The services and business processes included in the system architecture are represented through XML interfaces based on the Web Services Description Language (WSDL) [5] specification. Each XML interface presents the operations exposed by the service or business process, including the parameters needed for their invocation.

B. Security

The security in the communication between the system and the web server can be guaranteed using transport level or message level security. Many e-health systems offer transport level security basically to reduce the message size and to avoid the complexity of implementing encryption and signing software components at both communication channel ends. The main issue associated with transport level security is that the message could be changed at an intermediary point without detection, because it only offers point to point security in the communication channel using a HTTPS session between the requester and the provider. The HTTPS protocol encrypts all data between the requester and the provider using digital certificate present at the web server (Fig. 2) [6].

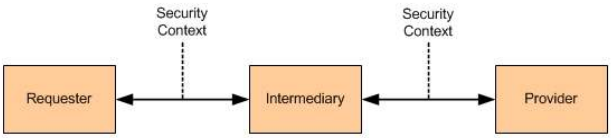

Fig. 2. Transport Level Security

In this proposal, message level security is implemented using the WS-Security standard for this purpose and the XML Encryption [7] and XML Digital Signature [8] W3C recommendations for message encryption and signing respectively. This approach ensures message integrity end to end because the messages are encrypted and/or digitally signed before the transmission. Only the recipient has the valid credentials to decrypt the messages using a keystore that contains the certificates exported by the message provider for message decryption. It facilitates detection of message changes during the transmission (Fig. 3) [6].

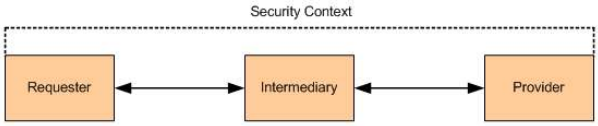

Fig. 3. Message Level Security

For each W3C recommendation mentioned, a separate keystore is used containing credentials to allow HL7 V3 messages interchange between system and web server (Fig. 4).

	XML Encryption		XML Digital Signature	
	Keystore	Certificate	Keystore	Certificate
HL7 Provider	TeleMedGICSender.jks	HL7AecgSender.arm	GICClientDS.jks	DGClient.arm
Web Server	TeleMedGICReceiver.jks	HL7AecgReceiver.arm	GICServerDS.jks	DGServer.arm

Fig. 4. Keystores and certificates organization

Fig. 5 shows the keys export/import approach implemented in the keystores used for XML Encryption. The same design was implemented for the XML Digital Signature recommendation.

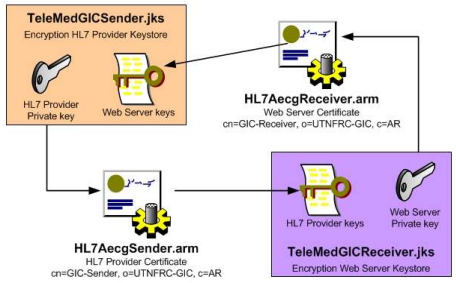

Fig. 5. XML-Encryption export/import keys approach

The *HL7AecgSender.arm* certificate is generated and imported into the web server keystore to have the keys needed to decrypt the messages transmitted by the HL7 provider. Same procedure is followed in order to decrypt the web server responses through the *HL7AecgReceiver.arm* certificate import into the HL7 provider keystore.

Although the WS-Security implementation implies an increase in message data size and time needed for processing, the system can be properly configured to transmit only medical study data needed for the specialist to make a first diagnosis, minimizing quantity and size of messages to be transmitted. It guarantees the confidentiality, integrity and authentication of the HL7 V3 message containing patient and medical study data in a more effective approach than transport level security using SSL protocol.

Fig. 6 shows the message data size increment associated with the XML-Encryption and XML-Digital Signature recommendations implementation.

C. HL7 V3 Messages

As the system processes ECG signals, the FDA (Food and Drug Administration Agency) XML format was selected, which is based on the HL7 V3 standard. Each XML element reflects a HL7 V3 reference implementation model (RIM) with the purpose of having all the information needed to

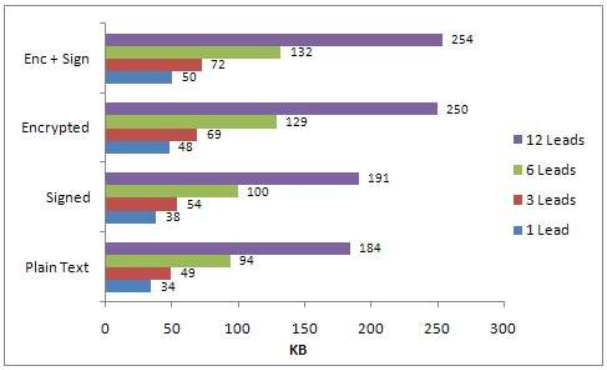

Fig. 6. HL7 V3 message size increase using WS-Security

construct a valid HL7 V3 message. A reference implementation model (RIM) is composed of a series of elements that can be acts (e.g. medical study) or entities (e.g. person or organization) who performs the mentioned acts [9]. The ECG signal information is represented by a *sequenceSet* act that contains a set of ECG leads acquired synchronously and each of them stored in an act named sequence. Regarding the base time, two elements are needed: *head* corresponding to the start date/time of the signal acquisition and *increase* that reflects the time duration of each sample, in relation with the signal sweep speed (0.002 for 25 mm/sec, and 0.001 for 50 mm/sec). Regarding the amplitude scale, the *origin* and *scale* factors specify the vertical scale resolution. The *digits* element results from dividing each digital sample by the *scale* element value per each lead from the acquired ECG signal. (Fig 7).

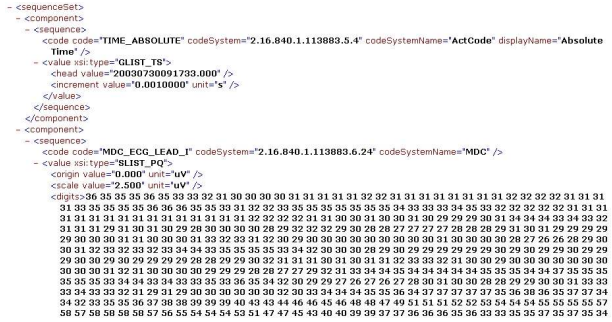

Fig. 7. ECG signal representation using the FDA XML standard

III. RESULTS

Using a portable ECG device that allows twelve sequential leads record and RS-232 connectivity [10], a series of five ECG studies was saved in one laptop to be transmitted through GPRS network using two different GSM modems. One of them uses 2G technology (Motorola G24 with RS-232 connectivity), while the other one supports 3G technology (Huawei E166 with USB connectivity). Each of them uses cellular phone network from different cell phone providers. Related to the security, four different configurations were implemented: without message level security (only HTTPS), signing, encryption and signing + encryption. In order to define the section for the acquired

ECG to be transmitted, the following parameters were specified: leads details, time in seconds per lead and scale. These parameters are set by the medical specialists in the request sent to the HL7 provider before message creation.

At the beginning, the parameters were defined in order to make a preliminary diagnosis for heart attack (5 seconds, 3 to 8 leads) and arrhythmia (10 seconds, 1 lead).

Fig. 8 shows a request using SOAP [11] protocol asking for a HL7 V3 message containing 6 leads with a duration of 10 seconds, using a 25 mm/sec sweep scale implementing signing + encryption as message security approach.

```
- <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:teleMed="http://teleMed.utnfrc.gic.com">
    <soapenv:Header />
  - <soapenv:Body>
    - <teleMed:customConfig>
        <teleMed:leads>I,V1,V2,AVR,AVL,AVF</teleMed:leads>
        <teleMed:scale>25</teleMed:scale>
        <teleMed:seconds>10</teleMed:seconds>
        <teleMed:security>Amachay</teleMed:security>
      </teleMed:customConfig>
    </soapenv:Body>
  </soapenv:Envelope>
```

Fig. 8. HL7 V3 message request using SOAP protocol

This configuration allows a reduction in the ECG signal size to be transmitted; it means reduce the number of characters for the XML tags associated with the ECG leads data in the HL7 V3 message. The other XML tags keep without changes independently of the parameters used per each transmission, because they are related to the mandatory HL7 V3 fields to represent the reference information models (RIM) related to entities like patient, location/time for the study and ECG device. The sample data includes a set of 32 tests with duration of 10 seconds using 25 mm/sec as sweep scale. These tests were executed in five different locations at different time of the day in order to check the system behavior in response to different available bandwidths in the cellular phone network. Each value in the Fig. 9 represents the average for 10 tests executed per each lead/security

	2G - Average Time in Seconds			
	1 Lead	3 Leads	6 Leads	12 Leads
SSL	6.438	8.432	8.621	12.785
Sign	12.030	14.670	17.207	26.305
Encryption	22.833	28.332	38.291	90.225
Sign + Encryption	23.954	29.396	40.253	97.017

	3G - Average Time in Seconds			
	1 Lead	3 Leads	6 Leads	12 Leads
SSL	2.041	2.266	5.719	8.151
Sign	2.156	6.766	7.891	10.531
Encryption	4.937	11.891	12.469	18.015
Sign + Encryption	5.923	13.469	13.515	25.031

Fig. 9. Average transmission time using 2G and 3G technologies.

configuration using 2G and 3G technologies.

Despite the increment of the transmission time associated with the GPRS network conditions, all of the messages were transmitted successfully.

In order to check if the HL7 V3 messages arrive to the web server properly, the tool named *XMLFDA Viewer* [12] was used to visualize ECG studies saved on HL7 Annotated ECG [13] format.

IV. Conclusion

This work has presented a system for secure HL7 messages transmission using GPRS network through message size optimization based on the customization of data needed to be transmitted.

According to the experimental results, this system provides a practical method to transmit ECG studies using HL7 Annotated ECG standard and web services security features for the generated messages.

Even though the system could transmit HL7 V3 messages using different communication systems, GPRS network was selected due its availability in remote locations without medical assistance infrastructure. In order to avoid that bandwidth restrictions prevent medical studies transmissions, a set of services were implemented having the objective of constructing HL7 V3 messages only with the medical data needed to make a preliminary medical diagnosis.

Through the addition of new services, the system architecture allows message setting in response to different medical diagnosis and additional HL7 V3 standards adoption for other medical studies.

References

[1] *V3 Messaging Standard, Health Level Seven (HL7) Standard, 2009.* Available: http://www.hl7.org/implement/standards/v3messages.cfm

[2] *Extensible Markup Language (XML), W3C Note, 2001.* Available: http://www.w3.org/XML/

[3] *Web Services Security (WSS), OASIS Standard 1.1, 2006.* Available: http://www.oasis-open.org/committees/wss/

[4] J. Voos, N. Viglieca and E.Gonzalez, "*Web based aphasia test using service oriented architecture(SOA)*", Journal of Physics: Conference Series, 2007. Available: http://iopscience.iop.org/1742-6596/90/1/012003/

[5] *Web Services Description Language (WSDL), W3C Note, 2001.* Available: http://www.w3.org/TR/wsdl

[6] G. Della-Libera, B. Dixon, J. Farrell, P. Garg, M. Hondo, C. Kaler, B. Lampson, K. Lawrence, A. Layman, P. Leach, J. Manferdelli, H. Maruyama, A. Nadalin, N. Nagaratnam, R. Rashid, J. Shewchuk, D. Simon and A. Wesley, "*Security in a Web Services World: A Proposed Architecture and Roadmap*", IBM Corporation and Microsoft Corporation, Available: http://www.ibm.com/developerworks/library/specification/ws-secmap/

[7] *XML Encryption Syntax and Processing, W3C Recommendation, 2008.* Available: http://www.w3.org/TR/xmlenc-core/

[8] *XML Digital Signature Syntax and Processing, W3C Recommendation, 2008.* Available: http://www.w3.org/TR/xmldsig-core/

[9] F. Badilini, L. Isola*"Freeware ECG Viewer for the XML FDA Format"*. 2nd OpenECG Workshop 2004, Berlin, Germany. Available: http://www.openecg.net/WS2_proceedings/Session05/S5.5_PA.pdf

[10] E. Gonzalez, F. Cagnolo, C. Olmos, C. Centeno, G. Riva and C. Zerbini *"Medical data transmission system for remote healthcare centres"* , Journal of Physics: Conference Series, 2007. Available: http://iopscience.iop.org/1742-6596/90/1/012029

[11] *Simple Object Access Protocol (SOAP , W3C Recommendation, 2007.* Available: http://www.w3.org/TR/soap/

[12] XMLFDA Viewer: tool for display and validate XML FDA aECG files. Available: http://www.amps-llc.com/XMLFDA.htm

[13] HL7 Version 3 Standard: Regulated Studies - Annotated ECG, Release 1, *Health Level Seven (HL7) Standard, 2004.* Available: http://www.hl7.org/V3AnnECG/