Building a Circle of Trust for the Virtual Hospital Network of the ALIAS project

Emmanuel EYRAUD\textsuperscript{a}, Thierry DURAND\textsuperscript{a}, Edouard BARTHUET\textsuperscript{b}, Romain BOCHET\textsuperscript{a}, Frédérique LAFOREST\textsuperscript{c}

\textsuperscript{a} GCS SISRA, Centre Léon Bérard, Lyon, France \\
\textsuperscript{b} Sword, F-69771 St Didier au Mont D'Or \\
\textsuperscript{c} Université de Lyon, CNRS INSA-Lyon, LIRIS UMR5205, F-69621 France

Abstract. The ALIAS project is aimed at linking together hospitals for sharing medical information and adopting telemedicine services to improve the efficiency of hospitals in Alpine Space areas. This article focuses on the circle of trust that has been set up among the partners of the project to address the security, authorization and identification issues of the project.

Keywords. eHealth, hospital network, circle of trust, information provision

1. Introduction to the ALIAS Virtual Hospital Network

With a society where people move more and more for personal or professional reasons, the biggest challenge is to provide the best quality of treatment all along the trips of the patient. The ALIAS [1, 2] project has decided to attack this problem by the setting up of a network of hospitals information systems or regional/national platforms dedicated to the exchange of EPRs. The implementation of such a network raises the need of a security bound to guarantee the confidentiality and the safety of patients' data.

Each hospital participating in the ALIAS Virtual Hospital Network (VHN) has a secured EPR system (EPRS) that allows the practitioners of this region to access information on the patients of the region. The ALIAS VHN is supported by the ALIAS Central Server (ACS). Active EPRS answer requests for clinical information they store. Passive EPRS are consumers of information exposed by active EPRS. The task of passive EPRS consists in identifying their users and granting them access to the VHN. Active EPRS also provide sensitive medical data within the circle of trust. Security issues related to sensitive data exchange are coarser.

2. Securing the ALIAS Virtual Hospital Network

Securing the entire VHN implies securing each node of the system. We have defined a shield in front of each partner. For a user to access a piece of information, a minimum of five queries/answers are exchanged between local EPRS and the ACS. We have

\footnotesize{1 Corresponding Author.}
protected our system with a reverse proxy twinned with a firewall (see figure 2). A query arrives at the entry of the ACS (A); it has been encrypted by the requesting EPRS in the VHN. The firewall pushes the message to the reverse proxy (B). The address of this proxy is known only by the firewall. The reverse proxy has the certificate to decode the message: it makes the message clear for the EPRS IHE connector. The proxy returns back the decoded message to the firewall (C). This “road backward” is only known by the reverse proxy. Before delivering the message to the regional EPRS, the firewall analyzes the message in order to be sure that is not a threat. Finally the message is delivered to the connector with no doubt on data integrity (D). On the way back, the ACS applies the same treatment.

Figure 2. Anti-intrusion security solution for the ALIAS Virtual Hospital Network

To sum up, the security of a network can be organized in three points:

- User authentication through logging in: this is the first and stronger barrier. An adequate strong logging system uses a chip card with a pin code or an OTP generator.
- User identity transmission within the circle of trust: the system must provide a normalized way of communication including the identity of the user, and keep traces of every actions done.
- Building a safe architecture: in the ALIAS project we have implemented reverse proxy and firewall technologies in front of each exposed system in order to grant the safety of the system and the confidentiality of the data.

The security architecture of the ALIAS VHN has reached the attended security level. Considering its applicability, non expensive hardware solutions are available on the market.

The final question that can be raised is how safe is this solution? Is it 100% hacker proof? No system can be 100% secure, but our architecture would require many efforts and a long time and we can assume that no one will be able to do it on his own.

Acknowledgments: This work is supported by the European Alpine Space Programme, under the project ref 4-2-2-IT. We thank all the partners included in this projects as well as the public healthcare authorities working as observers.

References