An architecture solution for security and interoperability of EHR systems

Mario Sicuranza, Mario Ciampi
ICAR-CNR, Via P. Castellino 111, 80131 Napoli, Italy
{mario.sicuranza, mario.ciampi } @na.icar.cnr.it

Abstract. The EHR allows obtaining a considerable amount of health information, to improve the quality and efficiency of medical care and at the same time to reduce the costs of health care. The strong interest on sharing the healthcare information in information systems over the years has led to development of many different and heterogeneous EHR systems. The increase of patient mobility requires the creation of a single (global) EHR system. In order to protect the investments made, the creation of a federated infrastructure which enables interoperability between different EHR systems and that ensures the security not only locally but also over the federated infrastructure itself is necessary. However, their intrinsic, high heterogeneity makes the attempt of their interoperability and security a hard task. This paper shows a general architecture to make different EHR systems interoperable and secure, thus showing how the issues of interoperability and security are exceeded when we define an interoperable infrastructure. This was experimented in the Italian region EHR systems to enable interoperability.

Introduction

The Electronic Health Record (EHR) is defined as a "digitally stored health care information about an individual's lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times" (Iakovidis, 1998). The EHR system (EHR-S) allows the obtainment of a considerable amount of health information that improves the quality and efficiency of medical care (Shekelle, 2006). The strong interest of the European Commission on the use of ICT in health, and in particular on the information systems for sharing the clinical information over the years has provided an opportunity for different stakeholders to develop their own information systems, but the different organizations have realized EHR solutions independently, obtaining in this way heterogeneous systems that do not interoperate among each other. Every information system produces clinical data independently and its documents are not easily accessible from the outside. Recently, the patient mobility has increased; always more patients receive medical treatments in areas that are different from where they live. This increase has imposed the urgent need of integrating local EHR-S so to realize the abstraction of a global EHR-S. In Italy there are various regional (local) solutions which are extremely heterogeneous (France, 2005), and almost all of these systems are based on the registry/repository paradigm, which requires the clinical documents to be archived in repositories and indexed in a registry. The goal is to have all medical documents available where patients are for receiving the best healthcare for their needs. There has been much investment in the existing regional EHR-S to redesign them anew, so the better solution is to enable interoperability between existing systems. Another issue in developing an interoperability solution is the need to ensure privacy and security. They are critical issues for local EHR-S, since the data stored or exchanged may contain very sensitive information, but, with the interoperable infrastructure, the complexity of the security issues increases. The aim of this work is to present how an architectural solution proposed in Italy and called InFSE (Technological Infrastructure of Electronic Health Record) can overcome the issues of interoperability and security. It allows to create a national federation of pre-existing regional EHR-S. InFSE architecture consists in a set of different Web Services components permitting the management, search and retrieval of clinical documents in all the national territory by creating a communication technology infrastructure (Ciampi, 2012).

Overview Architecture

Figure 1 illustrates an architectural overview of InFSE, which is structured as a multilevel service-oriented architecture:

- The lower level, called Connectivity layer, is represented by the Public Connectivity System (SPC), a technology infrastructure for the application cooperation among the Italian Public Administrations;
- The middle level is the Component layer, core of the architecture, that consists of the following software macro-components:
    - *Access Interface* is the interface of the federated infrastructure; it manages the interactions between heterogeneous EHR-S;
    - *Federated Index Registry* is a distributed component composed by the federation of regional registries; it allows the management of document metadata and enables the search of data managed by each local EHR;
    - *Document Manager* allows the storing and retrieval of documents;
    - *Hierarchical Event Manager* notifies clinical data to all interested users through a federation of brokers, based on the pub/sub paradigm;
    - *Access Policy Manager* is responsible for general security aspects.
- The upper level, named Business layer, defines the application services.

The secure interoperability between heterogeneous systems can be obtained through integration of pre-existing systems with the above components. The next two sections show the interoperability issues and security model, respectively.

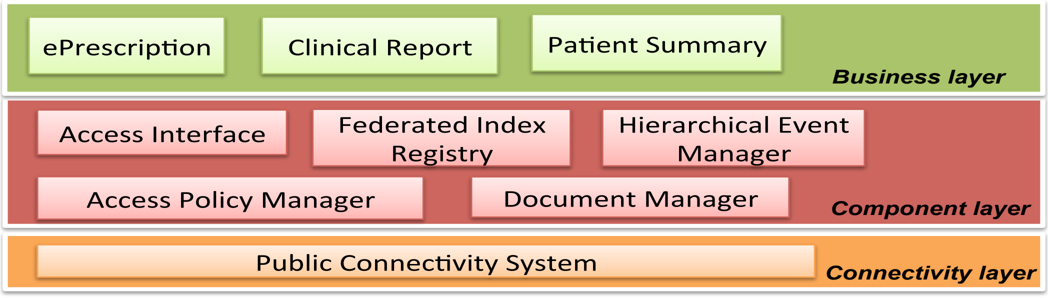

Figure 1. InFSE Architecture, structured as a three-level service-oriented architecture

Interoperability issues

The interoperability concern can be addressed by different levels, the Levels of Conceptual Interoperability Model (Tolk, 2003) can help in properly defining what kind of interoperability is needed. In an EHR-S, it is necessary to overcome the first four levels of interoperability, how InFSE overcomes these levels is described below. *Technical interoperability* is exceeded using standard communication protocols (HTTP, SOAP etc.). The definition of standardized communication interfaces (WSDL services), the use of open standards and the sharing of the data information model allows the overcoming of the *Syntactic interoperability*. The data model at the logical level is divided into two conceptual models; this division follows the registry/repository paradigm. The registry model is shared between different systems to ensure syntactic and semantic interoperability. The definition of the model follows the standard OASIS ebXML RIM specialized on the HL7 CDA 2 standard. The repository model does not need to be interoperable because every structure manages the clinical documents in their own way. *Semantic interoperability* is also exceeded with the use of shared coding systems (LOINC).

Security model

The *Access Policy Manager* allows to fulfil the security requirements such as Confidentiality, Integrity, Authenticity, Authorization, Non-Repudiation and Accountability. The used security model follows the principles of the WS-Security standard. The requirement of *Confidentiality* is achieved through the use of an encrypted patient identifier in order to keep personal data separate from healthcare information through the secure exchange message. Moreover, the access to data is controlled by the use of Access Control (AC). The solution provides an access control that follows the Attribute-Based Access Control model (Hai-bo, 2006). The requirement of *Integrity* is achieved using XML Signature that signs the SOAP message or part of it, and in this way also *Non-Repudiation* is guaranteed. To ensure *Authenticity* and *Authorization*, a portfolio of assertions (SAML assertions) that contains some attributes, such as user role and purpose of use is used. When the user makes a request to the service access, he/she associates with the request his/her portfolio of assertions. Our solution uses XACML to define and verify access policies based on roles and attributes. In this way, each local EHR-S is able to use its own policies. Finally, the requirement of *Accountability* is achieved through the logger made locally by services and the use of SPC.

Experimentation

The InFSE components have been integrated with different local EHR-S (regions and autonomous provinces). The integration operation achieves the same operations at the local level and furthermore it allows searching and recovering operations between systems involved. We experimented the InFSE infrastructure with the interchange of healthcare documents by interoperability of several regional EHR-S.

Conclusion

This paper briefly describes the InFSE solution that allows to develop a set of reference guidelines for the Italian domain. It defines the architectural model of an infrastructure to support interoperability and security of heterogeneous regional EHR solutions. As a future work, we are planning to define a set of services to provide patients the capability of specifying and managing the access rights on their health care documents in a dynamic and fine-grained manner.

References

Ciampi, M.; De Pietro, G.; Esposito, C.; Sicuranza, M.; Donzelli, P. (2012):"On federating Health Information Systems". International Conference on Green and Ubiquitous Technology pp.139-143.

France, G.; Taroni, F. and Donatini, A. (2005): " The Italian health-care system". Health Economics, vol. 14, pp. 187-202.

Hai-bo, S. and Fan, H. (2006): “An Attribute-Based Access Control Model for Web Services”. Proc. 7th Int’l Conf. on Parallel and Distributed Computing, IEEE, pp. 74-79.

Iakovidis, I. (1998): “Towards Personal Health Record: Current situation, obstacles and trends in implementation of Electronic Healthcare Records in Europe”. International Journal of Medical Informatics vol. 52 no. 128, pp. 105 –117.

Shekelle, P.; Morton, S. C. and E. B. Keeler (2006): "Costs and Benefits of Health Information Technology". Evidence Reports/Technology Assessments, No. 132

Tolk, A. and Muguira, JA. (2003):"The levels of conceptual interoperability model". *Fall Simulation Interoperability Workshop*. Orlando, Florida. Simulation Interoperability Standards Organization.