journal homepage: www.ijmijournal.com

Empowering citizens with access control mechanisms to their personal health resources

J. Calvillo[a,b,*], *I. Román*[a,b], *L.M. Roa*[a,b]

[a] *University of Seville, Spain*
[b] *CIBER de Bioingeniería, Biomateriales y Nanomedicina (CIBER-BBN), Spain*

ARTICLE INFO

Article history:
Received 23 April 2011
Received in revised form
15 February 2012
Accepted 15 February 2012

Keywords:
Distributed systems
Patient empowerment
Systems integration
Semantics
Medical informatics

ABSTRACT

Background: Advancements in information and communication technologies have allowed the development of new approaches to the management and use of healthcare resources. Nowadays it is possible to address complex issues such as meaningful access to distributed data or communication and understanding among heterogeneous systems. As a consequence, the discussion focuses on the administration of the whole set of resources providing knowledge about a single subject of care (SoC). New trends make the SoC administrator and responsible for all these elements (related to his/her demographic data, health, well-being, social conditions, etc.) and s/he is granted the ability of controlling access to them by third parties. The subject of care exchanges his/her passive role without any decision capacity for an active one allowing to control who accesses what.

Purpose: We study the necessary access control infrastructure to support this approach and develop mechanisms based on semantic tools to assist the subject of care with the specification of access control policies. This infrastructure is a building block of a wider scenario, the Person-Oriented Virtual Organization (POVO), aiming at integrating all the resources related to each citizen's health-related data. The POVO covers the wide range and heterogeneity of available healthcare resources (e.g., information sources, monitoring devices, or software simulation tools) and grants each SoC the access control to them.

Methods: Several methodological issues are crucial for the design of the targeted infrastructure. The distributed system concept and focus are reviewed from the service oriented architecture (SOA) perspective. The main frameworks for the formalization of distributed system architectures (Reference Model-Open Distributed Processing, RM-ODP; and Model Driven Architecture, MDA) are introduced, as well as how the use of the Unified Modelling Language (UML) is standardized. The specification of access control policies and decision making mechanisms are essential keys for this approach and they are accomplished by using semantic technologies (i.e., ontologies, rule languages, and inference engines).

Results: The results are mainly focused on the security and access control of the proposed scenario. An ontology has been designed and developed for the POVO covering the terminology of the scenario and easing the automation of administration tasks. Over that ontology, an access control mechanism based on rule languages allows specifying access control policies, and an inference engine performs the decision making process automatically. The usability of solutions to ease administration tasks to the SoC is improved by the Me-As-An-Admin (M3A) application. This guides the SoC through the specification of personal access control

[*] *Corresponding author at*: Escuela Técnica Superior de Ingeniería, C. de los Descubrimientos, s/n 41092 Sevilla, Spain. Tel.: +34 954 485 976.

E-mail address: jorgecalvilloarbizu@gmail.com (J. Calvillo).

doi:10.1016/j.ijmedinf.2012.02.006

policies to his/her distributed resources by using semantic technologies (e.g., metamodeling, model-to-text transformations, etc.). All results are developed as services and included in an architecture in accordance with standards and principles of openness and interoperability.

Conclusions: Current technology can bring health, social and well-being care actually centered on citizens, and granting each person the management of his/her health information. However, the application of technology without adopting methodologies or normalized guidelines will reduce the interoperability of solutions developed, failing in the development of advanced services and improved scenarios for health delivery. Standards and reference architectures can be cornerstones for future-proof and powerful developments. Finally, not only technology must follow citizen-centric approaches, but also the gaps needing legislative efforts that support these new paradigms of healthcare delivery must be identified and addressed.

1. Introduction

Nowadays it is widely accepted that the application of Information and Communication Technologies (ICT) in the healthcare environment leads to the improvement of care delivery, not only enhancing citizens' health but also including well-being and social care. Moreover, it increases subjects' quality of life and independence as well as reducing rising healthcare costs in an ageing society. Subject of care (SoC) centric approaches promote a personalized healthcare paradigm and represent a promising step forward. This paradigm could increase the involvement of the SoC in his/her own healthcare by encouraging him/her to take an active role in the management and maintenance of his/her health (e.g., by expressing concerns and preferences, participating in medical decision making [1], reinforcing the importance of lifelong learning and self-management, etc.). A requirement for an efficient personalized healthcare scenario is the integration of all the available knowledge about each SoC into a cohesive whole [2].

Most efforts focused on the promotion of the SoC as a proactive agent in his/her own healthcare are referred to the term “patient empowerment”. This topic covers a wide spectrum of approaches and solutions, but there is still a long road ahead. A hot point of discussion is about the ownership of the SoC's information and about who can decide policies to access it. National health laws [3], European directives and international recommendations [4–7] support that each individual must be able to control the information and resources related to him/her by avoiding unauthorized access. The trend is to involve the SoC not only in the maintenance of his/her health (through the awareness of all his/her information and resources) but also in the management and access control to them by means of the establishment of criteria that he/she considers adequate. This management paradigm of health resources (i.e., where the SoC is the absolute administrator and systems must ensure obedience to his/her preferences) is not easily achieved over currently deployed systems. If distribution and integration issues are considered, the accomplishment is even more difficult.

Several initiatives trying to bring the management of health resources to the individual the information of which they handle can be found [8–10]. One of the most relevant of these is the Personal Health Record (PHR) [11], indicated as an electronic application through which individuals can access to and manage their health information. Moreover, they can also share it with the person they authorize in a confidential, private and secure way. There are other examples such as the Person Controlled Health Record (PCHR) [10] or smart-cards scenario [12], where the information is carried by the SoC in a physical device and its disclosure is only up to the citizen.

Most of these examples focus on centralized scenarios where resources belong to a unique administrative domain, but this assumption is far from reality. Healthcare scenarios with distributed resources are not a futuristic approach. Nowadays any SoC has resources (information, dedicated devices, etc.) related to him/her within different health organizations across separate regions and even countries. A real SoC-centric approach should be seamless to the geographical and administrative locations of resources and spanned over any domain holding resources related to the SoC. Obviously this scenario complicates access management tasks, hence more sophisticated procedures of security administration are required.

Technology can ease the deployment of such paradigms and satisfy requirements of heterogeneity, distribution, and management by the SoC. Developers must not forget that if citizens have to design their own access policies, they must be provided with suitable tools. Therefore end-user applications have to be designed to ease their accessibility and use by the SoC, guiding him/her through understandable models and natural language and hiding the complexity of the computational languages for rule definition. Usability has been identified as a major asset to transfer the results of security and privacy research to practice in real systems.

In this paper, we introduce an open architecture following the principles of interoperability and system integration by using service-oriented architecture (SOA) [13] concepts and related standards. The proposed architecture supports a concept based on Virtual Organizations (VO) [14] that we have called Person-Oriented Virtual Organization (POVO). This concept emphasizes the definition of a VO, the objective of which is the health maintenance of an SoC who, furthermore, will also be the administrator. The POVO is a complex environment that involves many issues, and in this paper we address the access control management guaranteeing an essential security block. We stress the mechanisms of access control policy specification allowing the SoC to manage access to