➢ Title of the manuscript:

Easing the development of healthcare architectures following RM-ODP principles and healthcare standards

➢ Authors:

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

➢ Affiliation:

[a]University of Seville, C. de los Descubrimientos, s/n 41092 Sevilla (Spain)

[b] CIBER de Bioingeniería, Biomateriales y Nanomedicina (CIBER-BBN)

➢ Corresponding author:

J. Calvillo

Escuela Superior de Ingenieros, C. de los Descubrimientos, s/n 41092 Sevilla (Spain)

Tel.: +34 954 485 976

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

Abstract

RM-ODP has been widely accepted and used in the field of system and software model engineering and of enterprise computing within different environments. One of these specific domains is healthcare, in which the international standard Health Information Services Architecture (HISA) is applied under the directives of RM-ODP. HISA presents a flexible architecture identifying common use cases, actors, information, and services and easing its extension with specific services, systems and information. The HISA standard follows system specification through the RM-ODP viewpoints but it does not consider other features of the reference model, such as the Enterprise language or the UML4ODP specification.

In this paper, we introduce the rationale and specification of the three technology-independent viewpoints of an HISA-based architecture conforming to RM-ODP and UML4ODP. Moreover, we evaluate how easy it is to extend this architecture to introduce specific services and elements. As proof of concept we explore security and privacy issues (i.e., requirements, actors, information objects, etc.) and enrich the architecture with suitable objects and services, mainly from access control standardization efforts. In addition, a detailed discussion about the divergences between RM-ODP and HISA is presented.

The main contribution of our work is to develop (guided by RM-ODP, HISA, and other standards) a methodology and tools allowing healthcare service developers and designers to build solutions conforming to standards and leveraging the benefits of distribution and interoperability. These tools consist of the specification of three technology-independent viewpoints according to the guidelines of HISA, RM-ODP and UML4ODP for the healthcare domain, and they will be freely available. In parallel, these viewpoints are extended with access control issues, and the adequacy of the HISA extension mechanism is evaluated.

Keywords: healthcare information systems; RM-ODP; HISA; security; access control

1. Introduction

Nowadays it is widely accepted that the application of Information and Communication Technologies (ICT) to the healthcare context leads to the improvement of health and social care delivery. This enhancement increases the quality of life and independence of citizens as well as the reduction of costs. Traditional developments of ICT solutions are centered on particular requirements and use cases. Moreover, they tackle each specific problem as isolated from the whole healthcare organization. This results in a lack of flexibility, scalability and reusability. Consequently, solutions can only be used in the particular context for which they were designed. This situation often occurs in the healthcare context where a wide spectrum of devices, systems and services exists. Each element is focused on a specific problem implementing heterogeneous, often proprietary, technologies, and with little or no possibility of interoperability with others.

Due in part to the application of ICT to this domain (electronic health record (EHR), ubiquitous monitoring, etc.), current healthcare delivery is evolving from using the physically available information at the point of care to synthesizing all the knowledge about each person into a cohesive whole, no matter where it is stored. This evolution requires the consideration of distributed scenarios instead of centralized ones. Moreover, distribution must be accomplished across organizational boundaries because any location where health and well-being care could be delivered (or information could be stored) should be included.

In parallel, healthcare stakeholders (i.e., national authorities' representatives, ICT solution providers, researchers, health professionals, patients, healthcare providers, and so on) have expressed their commitment towards the deployment of interoperable eHealth services providing the optimal personalized care. However, achieving this new healthcare scenario is not easy. New generation healthcare services must be built over strong foundations facilitating reuse, interoperability and scalability. Thus, they could take advantage of the synergies among them in order to offer the optimal personalized end services to the users. At the same time, the huge complexity and heterogeneity of scenarios must not be underestimated, considering the broad range of social, health and well-being care categories.

A major barrier to the realization of the new healthcare delivery is that the integration, interoperability and reuse of services are complex tasks in such an evolving and heterogeneous context. Although standardization is a cornerstone for interoperability, capabilities and knowledge managed by services are heterogeneous in their nature. Only through the deep understanding of the overall architecture can an effective integration and composition of services be achieved. A healthcare architecture could be defined as a formal description of a system providing well-being, social and health care services. This description is organized in a way that it could even support reasoning about the structural properties (i.e., relations between elements) of the system. It defines system components, or building blocks, and provides a plan from which products can be procured and systems developed according to the goals and requirements. Those components will work together to implement the overall system. By conforming to international norms, formal languages, and standard methods, a normalized reference architecture could be provided to guide stakeholders in their decisions and activities, helping to solve integration issues.

The consensus among stakeholders about the best methods for the effective and practical application of architectural principles is critical to provide a reference framework. Such a framework must establish, in a comprehensive manner, the set of standards, methods and best practices for the development, validation, and even certification of advanced services and applications. It must consider the most relevant innovative infrastructures and basic health services, reusable in different use cases. It is also necessary to identify gaps in standards and methods that need to be bridged to walk the road ahead. This framework would be the pillar for the design of innovative infrastructures that could lead to a competitive position for the delivery of affordable scalable well-being, social and health care services, opening new valuable business lines for the provision of the best personalized care.

The vision of a healthcare environment as a cohesive whole will allow future solutions to cooperate in order to reuse capabilities and accomplish more complex goals. Moreover, a more efficient and personalized healthcare delivery will be eased by integrating all the knowledge related to one single person (from diagnosis and treatments to daily life, genomics and monitored data). Thus, each particular solution will be a building block of a bigger system (the healthcare domain) that will be evolvable and more and more complex, sophisticated and efficient. The International Standard ISO 12967 "Health Informatics – Service Architecture" (HISA) [1] and other architectural approaches particularized to the healthcare domain, such as the Service Aware Interoperability Framework (SAIF) [2] or the NEHTA Interoperability Framework [3], are regarded as valuable starting points to pave this difficult path.

In this paper we introduce two important contributions to the standardization of a framework for the design and development of healthcare distributed services promoting openness, interoperability, reusability and scalability. The first one is the reinforcement of HISA by promoting the adoption of architectural principles through the formalization of its viewpoints by using the ISO 19793 standard (UML4ODP) [5]. The second one is the refinement and extension of HISA to cover security issues considering the main standard references in this matter. The latter could be considered as a proof of the concepts introduced in the first one, since we use the ODP formalization as a base for this work. As HISA only specifies the three technology-neutral viewpoints of RM-ODP, the contributions are totally independent from specific platforms, ensuring its survival across time.

The rest of the paper is organized as follows. In Section 2, we introduce the main hypothesis, theories, methodologies, and also CASE tools used as the basis for the development of our work. We place special emphasis on the role of HISA and RM-ODP in healthcare architecture work. Moreover, security and access control issues are considered as HISA extensions. In Section 3, the results of our research are exposed as well as the main aspects required to solve the formalization of HISA using UML4ODP. It is also explained how this specification has been used as an initial point for the formalization of security services and processes. Section 4 is centered on the divergences between HISA and RM-ODP and the difficulties found in the extension of HISA. Moreover, we also discuss our medium and long-term viewpoint on the practical assumption of architectural matters in healthcare environments. The paper ends with some concluding remarks.

2. Material and Methods

2.1 Architectural Issues in the Healthcare Domain

Considering the heterogeneity and complexity of services supporting health delivery, there is a growing need to interconnect health information processing systems [6]. More and more current organizational processes demand information exchanges within and between multiple healthcare organizational domains, which means that systems must work in a distributed computing environment. The design, development, deployment, maintenance and evolution of a distributed system are highly complex tasks. Consequently, it is essential for an architecture (and any function necessary to support it) to be defined through a set of standards. Some healthcare architectural approaches have been developed by standardization organizations like the European Committee for Standardization (CEN) [7], the International Organization for Standardization (ISO) [8] or the Object Management Group (OMG) [9].

The three-part International Standard ISO 12967 “Health informatics - Service architecture” (HISA) [1] is one of the most relevant efforts to specify a reference architecture in the healthcare domain. The purpose of the HISA standard is two-fold; it must:

- Identify a framework to describe healthcare information systems through languages, notations and paradigms suitable for facilitating the planning, design and comparison of systems. RM-ODP [6] has been selected as the reference model.
- Identify fundamental architectural aspects (workflows, information and services) enabling the openness, integration, interoperability and scalability of healthcare information systems.

This standard evolves from the European standard set ENV 12967, which has been the basis for several implementations of middleware products and integration efforts in regional healthcare information systems [10]. The ISO 12967 takes into account the experiences from the practical use of the ENV as well as other architectures and health infrastructure initiatives carried out by CEN, and their alignment with the large body of information model standards developed in support of various communication purposes.

RM-ODP is an important basis for the production of ISO 12967 (it has been selected as the architectural framework), but only the three technology-independent viewpoints (i.e., Enterprise, Information and Computational Viewpoints) are used to produce the HISA standard. Thus, an open and technology-independent design of the architecture is promoted. The two technology-dependent viewpoints should be considered in a specific implementation context and consequently they are not standardized.

RM-ODP defines concepts for a formal specification of any distributed system, but it does not force a formal modelling notation for representation. The description of the Enterprise, Information and Computational Viewpoints has to be expressive enough to faithfully represent all the necessary concepts. Formal specification languages such as the Unified Modelling Language (UML) have been traditionally used to represent architecture viewpoints. The Recommendation | International Standard X.906 | ISO/IEC 19793 (commonly known as UML4ODP) [5] aims to use UML as a modelling notation for RM-ODP specifications, addressing issues identified in previous research work [11-13]. UML4ODP defines the use of UML 2.1.1 to specify open distributed systems in terms of the RM-ODP viewpoints. It defines a set of UML profiles for the expression of such specifications and an approach for structuring them according to RM-ODP principles. An additional purpose of UML4ODP is to allow developers to use UML profiles to write ODP specifications and to be able to process them by means of UML tools. An example of a CASE tool is the combination of MagicDraw®

[14] and the RM-ODP plug-in [15] developed by the Atenea Research Group [16], which was used in this work. The ISO 12967 standard does not force the use of UML4ODP, but this paper will show its use for the formalization of the HISA-based architecture.

Several researches in this area have recently been undertaken by CEN working groups related to architectural issues. The authors will try to make public their models as technical guidelines under the protection of Standard Development Organizations (SDO), in order to give designers and developers practical tools helping them in the development of solutions compliant with the HISA standard.

Finally, it is interesting to point out other initiatives in this field. The Service Aware Interoperability Framework (SAIF) [2] tries to organize and manage architectural complexity with a set of constructs, best practices, processes and categorizations. It combines four sub-frameworks (Information, Behavioral, Governance, and Enterprise Conformance and Compliance) for defining and managing comparable interoperability specifications. Another effort is the Interoperability Framework (NEHTA IF) [3] developed by the Australian government to address interoperability issues in the eHealth domain. The NEHTA IF provides a key set of architecture abstractions and guidelines for collecting requirements and developing eHealth specifications. Both SAIF and NEHTA IF are directly based on the RM-ODP foundations, using concepts established by the framework, and in conjunction with other initiatives such as MDA or HL7 artifacts. Thus, they should be taken into account as examples of how to align an approach with RM-ODP. Another initiative, although not related with RM-ODP, is the Healthcare Services Specification Project (HSSP) [4] whose objective is the identification and documentation of service specifications, functionalities and conformance support relevant for stakeholders of the healthcare domain. HSSP places emphasis on implementations and its outcomes are strongly aligned with the MDA philosophy, using UML as a formalization tool. Some contributions from these initiatives relevant to future HISA versions will be analyzed in the discussion section.

2.2. Security and access control issues

As introduced above, one of the key issues to ensure the openness and interoperability of solutions is the adoption of standards in both the general and healthcare domains. Security has been the focus of significant effort by SDO and other organizations. In the generic domain, one of the most relevant initiatives is the ISO/IEC 10181 standard [17], the scope of which is to describe the organization of security frameworks and define common security concepts. Other well-known efforts are: the X.509 recommendation from ITU-T [18][19], defining a public-key and attribute certificate framework; several IETF RFC (Request For Comments) [20] related to security issues such as the 2828 [21] and 3198 [22] RFCs, giving internet security glossaries and showing a security framework for internet use; and the standards published by OASIS [23]: the eXtensible Access Control Markup Language (XACML) [24] and the Security Assertion Markup Language (SAML) [25]. Similarly, the healthcare domain has its own approaches and recommendations. In particular, the ISO/TS 22600 standard [26] is intended to support the needs for healthcare information sharing across unaffiliated providers, organizations, insurance companies, subjects of care and so on. It supports collaboration among authorization managers that may operate over organizational and policy borders. It introduces the underlying paradigm of formal high level models for architectural components based on RM-ODP.

In previous work [27], a harmonization of these and other security standards was performed in order to extract common architectural features that were suitable for modelling within a HISA-compliant architecture. Among other features it can be pointed out, for example, that the authentication and authorization tasks are tackled separately; or that the functions for access control are usually decomposed into Policy Enforcement Points (PEP, also known as Access Control Enforcement Functions) and Policy Decision Points (PDP, also known as Access Control Decision Function).

A relevant schema for access control is the attribute-based model(ABAC), in which attributes can be assigned to subjects and access privileges are not directly related to subjects, but to attributes, easing management tasks and scalability. The ABAC model is a generalization of the widely accepted role-based access control model (RBAC) in which an attribute is restricted to an organizational position or role. ABAC is more flexible because an attribute can be any feature of the subject such as his/her professional category or the place where he/she lives.

The access control discipline is used in this work as a test for the HISA extension mechanism. This issue has been chosen due to both its relevance in healthcare architectures and the experience of the authors in this field.

3. Results

Section 1 has established the current context and concerns of system engineering applied to the healthcare domain. HISA has emerged as a relevant reference in this field but it is not gaining so much momentum as was previously expected. We make the assumption that should HISA be more aligned with RM-ODP (not only in the separation of concerns through viewpoints), the application would be easier and more widespread. To test this hypothesis, in the current work we have refined the formalization of the three technology-independent viewpoints of an HISA-based architecture conforming to the RM-ODP framework and the UML4ODP standard. Requirements and normative references from the HISA standard have been specified according to RM-ODP. These results and the HISA methodology for extensions have been validated by means of the extension of HISA with security concerns. In this section, the outcomes are briefly presented with respect to both HISA-based architecture and security extensions. During the specification process several difficulties have been found and these are explained in Section 4.

3.1 HISA Specification Conforming to RM-ODP

Next we describe the viewpoints of our HISA-based architecture. For the sake of clarity, the complete specification has been omitted in this paper but it can be obtained from [28].

a) Enterprise Viewpoint

The normative parts of the HISA standard for this viewpoint are: an overall schema with the main enterprise objects and their relations, a set of general requirements, three workflow requirement sets (i.e., subject of care, clinical information and activity management workflows), and requirement specifications for clusters of users' activities (i.e., resource management, user and authorization management, and classification, coding and dictionary management activities). All these normative points have been specified in the HISA-based architecture by using modelling concepts from the UML profile for the RM-ODP Enterprise Viewpoint.

Firstly, a community called the ***Healthcare Information System*** (HIS) has been specified. Its objective, extracted from the strategic paradigm of HISA, is to support health care, organizational and managerial activities within a health care organization. It has been considered that this community is composed of an aggregation of communities, thus a community has been specified for each workflow and cluster of activities. These communities are only refinements of the different areas of the HIS community. The second point consists of the identification of roles and actors and the assignment rules within the HIS community. From the HISA specification, a role has been specified for each workflow and cluster of activities although more roles could be established with a further development of each community. Moreover, other enterprise objects (such as ***PatientPlan*** or ***Resource***) have been identified. Finally, four enterprise policies have been defined according to requirements directly extracted from the HISA Enterprise Viewpoint. These are ***identification of subjects of care, non-duplication of clinical information*** and ***authorization profiles for users and resources***. The extraction of policies from the HISA standard presented serious difficulties as is explained in the Section 4.

b) Information Viewpoint

The HISA Information Viewpoint specifies several UML class models identifying information objects as well as required attributes for each one. In the current work, the Information Viewpoint of our architecture is composed of an invariant schema for each UML model defined in HISA. Thus, we obtained a high-level schema of information objects, two of metamodelling (i.e., ***generic HISA class*** and ***classification objects***), and six corresponding to workflows and clusters of activities. According to RM-ODP an information viewpoint can also contain static and dynamic schemas but these cannot be extracted from HISA, as is discussed in Section 4.

c) Computational Viewpoint

The third part of the ISO 12967 standard describes three types of computational objects: basic, general-purpose, and complex. Each one has a set of generic methods, a scope and a textual description. The specification of these requirements in our architecture has resulted in one model including the three kinds of computational objects, their methods and interfaces. Moreover, a basic computational object has been identified corresponding to each information object, and all these have been specified in several models.

Obviously, this viewpoint has to be significantly extended in practical applications of HISA. Likewise we recommend the extension of this part (such as the previous one) on the basis of considering other standardization efforts.

d) Viewpoint correspondence

As is discussed below, HISA does not explicitly describe correspondences between the Enterprise and Information Viewpoints, but some relations between objects can be extracted. A package stereotyped "***CorrespondenceSpecification***" contains nine "***CorrespondenceLink***" between enterprise and information objects (see Figure 1). In addition, HISA establishes the correspondences between the Computational and Information Viewpoints. Each basic computational object corresponds to an information object, and complex computational objects to workflows and cluster of activities. These correspondences have been established in another package.

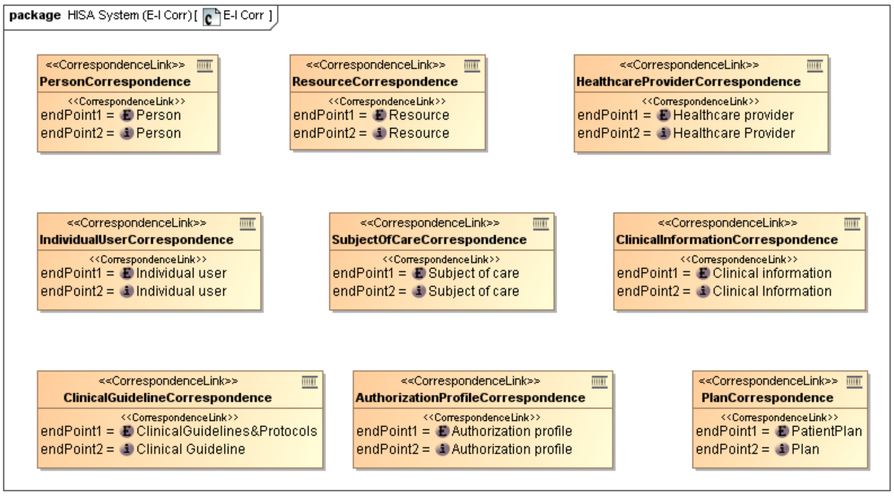

Fig. 1. Correspondence specification between the Enterprise and Information Viewpoints

3.2 HISA extension: security and access control

The feasibility of expanding HISA has been studied by including normalized concepts of security and access control in the architecture. Moreover, this work serves as a test of the suitability of the formalization developed above for the HISA standard conforming to RM-ODP and UML4ODP. The concepts, actors and processes of access control have been extracted from a harmonization of standards and initiatives presented in previous work [27].

The community HIS contains the whole specification of the architecture defined by an aggregation of communities. Within this set, a new community called ***Security Infrastructure*** was included to specify separately security issues. The choice to create a separate community is due to the precise definition of the concept. According to RM-ODP, a community is a configuration of objects modelling a collection of entities (e.g., human beings, information processing systems, resources of various kinds…) that are subject to some implicit or explicit contract governing their collective behavior, and that has been formed for a particular objective. Thus, in order to promote the modularity and scalability of the formalization, we decided to concentrate all security issues in one community. Although in this work we focus on access control, any security issue could be included in this community. The current objective of the Security Infrastructure community is to manage user privileges and attributes and to control the access to resources based on policies. Some of the processes identified in the Enterprise Viewpoint are ***Add user***, ***Edit policy***, ***Grant attributes to user***, or ***Make access control decision***. Examples of roles are ***Decision agent*** (played by the entity responsible for access control decision), ***Policy Admin*** (manager of policies) or ***Requester*** (entity requesting access to a resource). Finally, the enterprise objects of this community have been mapped from the harmonization of standards. Thus, there is an object (***Policy Enforcement System***) related to normalized PEP and another (***Policy Decision System***) correspondent to PDP.

The Information Viewpoint is composed of the concepts and relations specified by the HISA standard and those included and related to security are mainly extracted from well-known standards. Figure 2 shows an information model as an example of this viewpoint. The model represents the information objects of the user and authorization management activities specified by HISA. To this set of objects (inside the red boundary) we have added those related to access control such as ***Access control decision*** or ***Attribute***. The HISA information objects not directly linked to ours are hidden for the sake of clarity. Some examples of integration relations between HISA and security extension are: an ***Authorization profile*** composed of, at least, an ***Access control policy*** and managed by a ***Policy information system***; and an ***Access control decision*** made by a ***Policy decision system*** and linking a ***User*** and a ***Controlled element***.

Finally, the extension to the HISA Computational Viewpoint is performed by establishing one computational object for each information object related to security. When including the computational objects for access control, the requirements from the third part of HISA must be taken into account. The systems involved in the access control processes are defined here as computational objects and their methods grouped in interfaces. In this viewpoint, standards such as XACML and SAML are very useful as a common ground for establishing protocols and interfaces. A potential risk in this point is to carefully separate the applied recommendations (e.g., XACML) from specific technologies (e.g., XML), which will be specified in the Engineering and Technology Viewpoints but not here. In addition to access control issues, the current version of this viewpoint should also be extended with infrastructure objects (common to advanced architectures) to become a proper reference model. There are numerous architecture standardization efforts that could serve as starting points and some examples are introduced in Section 4.

In this paper, security issues have only been used to identify pitfalls and opportunities for the HISA extension mechanism. Hence, the complete specification of the extension is not included here but it will be the focus of future work.

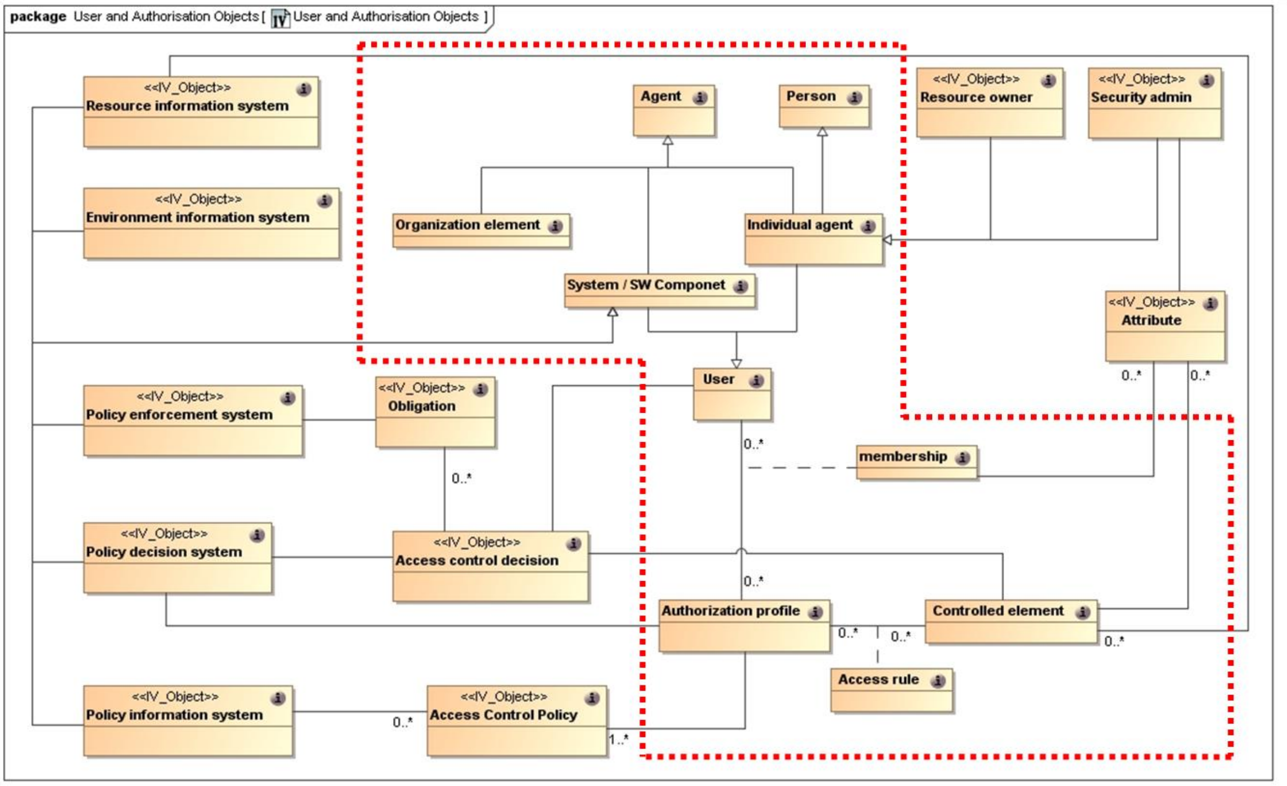

Fig. 2. Example of an Information Viewpoint model integrating HISA objects with access control concepts

4. Discussion

4.1. HISA and RM-ODP: Alignments and Divergences

The first version of HISA was published in 1997 and described an architecture to be applied within the healthcare domain following directives of the RM-ODP framework. Meanwhile and after ten years of public use and feedback, the ODP reference model had become a mature effort of standardization with wide dissemination and acceptance in the industry and academic fields [29][30]. From the beginning, HISA adopted the separation of concerns by means of viewpoints, inheriting one of the most useful features from RM-ODP and international recommendations [31]. However, HISA does not aim at being a complete and close set of specifications but an open and evolvable architecture. Thus, it only formalizes specific features identified as common and essential within any advanced healthcare information system. As a consequence of this flexibility, certain areas are not covered in detail such as, for example, security issues [32].

During the ten years of HISA as a European pre-standard, several works [33][34] have pointed out weak features such as a diffuse separation between the Enterprise and Information Viewpoints or the difficulties to distinguish normative parts from informative ones. Many of these points were tackled for the final release of this standard, however the application of HISA still remains far from that of RM-ODP, always considering the different scopes of both frameworks. Obviously, a major barrier for the application of such a paradigm is the inherent complexity of the healthcare environment, as was stated in Section 1. Apart from the context of HISA and RM-ODP, it could be assumed that if HISA were more aligned with RM-ODP, maybe its application would be easier and as widespread as RM-ODP is. In this paper, we have studied this hypothesis by promoting the RM-ODP guidelines and formalizing the HISA specification according to them. The main similarities and divergences between these two standards (without forgetting their different scopes) are presented below. Our aim is to provide a starting point for useful discussion about potential evolutions of the HISA standard.

The first divergence that an architect finds is the methodology of viewpoint specification. RM-ODP does not prescribe a particular process for specification of viewpoints, delegating this decision to the architect. This point has been criticized in some works [35] and there have been approaches to combine RM-ODP with known methodologies or to construct new ones oriented to the framework [36][37]. The HISA standard covers the development process by establishing a methodology in two parts. The first one has the strategic paradigm as source of the Enterprise, Information and Computational Viewpoints. This document aims at being concise, managerial-oriented and it identifies overall requirements and strategic objectives of the envisaged system. The Enterprise Viewpoint is specified from the strategic paradigm, and the Information and Computational Viewpoints are detailed in a cascade process. The second part of the HISA development process is an iterative specification detailing each viewpoint through multiple, subsequent levels of refinement.

The flexibility of RM-ODP can make an architect choose the most intuitive methodology to specify systems, i.e. in cascade from platform-independent viewpoints (Enterprise, Information, and Computational) to those platform-dependent (Engineering and Technology). Although this methodology is the most intuitive, it may not be the most appropriate. Or maybe HISA should be more flexible and as development-process-neutral as RM-ODP. Further work is required in order to conclude which methodology is the most suitable for HISA and which one for RM-ODP (or for both). To the authors' experience, an iterative refinement process seems to be more appropriate a priori, since it allows the initial specification of common features of the healthcare domain and, in successive refinements, to develop them in depth. This could be the most suitable specification process according to the size and complexity of such a domain.

The second point to discuss is about the notation and formalization languages. RM-ODP was released without a normative reference to modelling languages. The Enterprise language appeared four years later [38] and the ISO 19793 in 2007[5] (ten years from the publication of RM-ODP). This lengthy wait for a normalized notation explains, at least in part, why HISA presents an informal format for requirements related to viewpoint specification languages. Indeed, the HISA standard does not prescribe the adoption of any specific modelling notation although the utilization of UML is recommended. We think that pure text and UML diagrams can be useful for small and simple architectures but it is unfeasible to cover a flexible, future-proof and complex healthcare system with them. Furthermore, the use of normalized notations allows the reduction of management tasks during the life cycle of systems and also eases specification interchange and interoperability among organizations and stakeholders.

HISA does not consider the Enterprise language and the UML4ODP standard as normative references but only as bibliography of interest. In this work, we have transferred the requirements and normative specifications of the HISA standard to a formalization conforming to RM-ODP, the Enterprise language, and UML4ODP. Due to the enormous flexibility of RM-ODP for accommodating a wide range of information systems and its precise notation by using the UML profile of the ISO 19793 standard, the formalization of the HISA requirements and specifications through UML4ODP has been quite simple.

The only possible misunderstanding can appear in the translation of requirements from pure text to Enterprise Viewpoint policies. The HISA informal description of requirements, mainly in the Enterprise Viewpoint, makes it difficult to clearly understand which requirements are mandatory and which ones are simple recommendations or context examples. In our work, we identified four main requirements and formalized them as policies. These are related to the identification of subjects of care, the non-duplication of clinical information, and the authorization profiles for users and resources. A few more requirements can be extracted from the HISA standard but their modelling implies the introduction of enterprise objects and processes that are not explicitly considered in HISA. Although these requirements cannot be modeled by Enterprise Viewpoint policies, they will have to be satisfied by the architecture implementation (i.e., Engineering and Technology Viewpoints), which is out of the scope of the HISA standard.

Another consideration from the formalization stage is the correspondence specification between viewpoints. The viewpoints are not independent from each other and they refer to the same architecture. Thus, correspondences between viewpoints should be formally stated. ISO 12967 describes a few relations between the Enterprise and Information Viewpoints only, and they are always formatted in plain text. For example, the clusters of objects are refined, and a mapping between the enterprise and information objects is implicitly suggested. Correspondences between the Information and Computational Viewpoints are more explicitly established. In general, HISA does not pay enough attention to this feature of architecture formalization, which would result in a coherent and integrated specification, with all the viewpoints working together and without inconsistencies.

Unlike HISA, the specification of correspondences between viewpoints is one of the strong points of RM-ODP as it has been praised in several works [39][40]. RM-ODP states that a complete specification of any system should include statements of the correspondences between the terms and language constructs relating one viewpoint specification to another. RM-ODP only describes generic correspondences between the Computational and Information Viewpoints, and between the Engineering and Computational Viewpoints. For the rest of the viewpoint pairs, correspondences will depend on the specifications of the particular system. The notation of correspondences is widely covered in the UML4ODP standard by means of the introduction of the concept of a correspondence link. The application of this notation to formalize correspondences between HISA viewpoints is an easy task because of the simplicity of the viewpoints. Firstly, the mapping of enterprise and information objects is straightforward due to the fact that both viewpoints are built from the same high-level object model the source of which is the strategic paradigm. Moreover, the Computational Viewpoint exclusively describes generic objects and interfaces, but they have to be in correspondence with the information objects, although the HISA standard does not establish this requirement explicitly. Besides that, the formalization and explicit representation of the correspondences between viewpoints is a precise mechanism to maintain consistency and coherence of specifications, and HISA could adopt it easily.

Once a system is specified and implemented, its conformance with the HISA standard and the specification must be tested. In addition to correspondence definition, the overall conformance testing process is another point of divergence between HISA and RM-ODP. The former indicates that a formal specification of the information system of a healthcare enterprise shall conform to the methodology and shall consist of the mandatory documents defined in it (i.e., the strategic paradigm and the Enterprise, Information and Computational Viewpoints). The specifications of the Engineering and Technology Viewpoints are optional. Moreover, a system conforming to HISA will have to implement all the information objects and to provide all the computational services defined in this standard.

On the other hand, the RM-ODP framework identifies conformance points within the set of viewpoint specifications at which observations of conformance can be made. It also defines classes of conformance points and it specifies the nature of conformance statements to be made in each viewpoint and the relations between them. A reason why HISA does not adopt these conformance points is because they are mainly defined in the Engineering Viewpoint, and HISA only establishes the three technology-independent viewpoints as mandatory. Hence, with the current version of the HISA standard, conformance can only be observed in the Enterprise, Information and Computational Viewpoints, but not in the implementations with middleware. The authors consider that HISA could provide explicit guidelines for conformance testing of implementations, but it is not clear whether RM-ODP conformance points are the most suitable mechanisms for the HISA standard.

Finally, the last comment about the comparison of HISA and RM-ODP is the standardization of infrastructure services. According to the identification of basic services, RM-ODP defines functions that are fundamental for the construction of any ODP system. These functions are base architectural services that will be included in the implementation design. They are grouped in the following areas: management, coordination, repository and security. So far, only two functions are standardized (trading function [41] and type repository function [42]) but all of them are considered, expressed by interfaces and stereotyped “NV_X”, where X is the name of the function, in the UML profile of the Engineering Viewpoint defined by the UML4ODP standard. Although these functions are not prescribed in the ODP framework, we consider that their identification is a starting point that HISA should adopt. Instead of that, the ISO 12967 standard does not mention them at all. The authors consider that these functions are common and essential for any ODP (and thus, HISA) system, and the standardization, or at least identification, of them could avoid future concerns among isolated systems due to disparate support functions.

4.2. Extending HISA: Chances and Pitfalls

Focusing on the ISO 12967 standard and leaving aside its commonalities and differences with the RM-ODP framework, HISA is an effort that offers a wide range of future possibilities. This enormous potential could lead HISA to be a relevant reference for industry and academia, but an identification of pitfalls or weak points is required to ease its application. The remainder of this section is devoted to these weak features.

Firstly, HISA normalizes a set of objects, within the Enterprise and Information Viewpoints, which are commonly required in any information system of a healthcare enterprise. These definitions are useful to establish a common reference frame easing interoperability between products and middlewares. A potential problem is that the specification of those objects is not complete enough. For example, the invariant schemas of information objects are formalized but there is no reference to the static schemas of the architecture or the dynamic schemas of those objects. The authors consider that this is a key point that could be developed in detail because of the importance of understanding the different states which the information objects can have. Some objects (e.g., ***Agent*** or ***Resource***) may not have a unique and defined set of states and their interpretation could vary from one implementation to another. In these cases, it is understandable not to specify a particular group of states. Other cases such as the ***Activity*** information object require that specification. This element has its corresponding in the Enterprise Viewpoint and there a set of states is defined, specifically ***foreseen***, ***requested***, ***accepted***, ***terminated*** and more. It is important to cover all the parts of the HISA standard since the frontiers between the Enterprise and Information Viewpoints are diffuse in some cases.

A second example of mixture between viewpoints that could lead an architect to problems to an architect is the fact that some basic processes are identified but not normalized. According to the Enterprise Viewpoint, HISA specifies requirements and information attributes focused on the management of information; in particular, these attributes are related to version control, auditing, and management of the life cycle. An architect could think that by adopting these sets of attributes, he/she is covering the correspondent functionalities, and his/her architecture will be interoperable with other systems conforming to HISA. But this thought could be wrong. Actually, without a precise definition of the processes related to version control, auditing, and management of the life cycle, a complete interoperability between solutions cannot be assured, even though they adopt the normative attributes of the HISA standard. Hence, we consider that an architect should start by extending HISA with the features identified but not normalized. In this particular case, it would be necessary to formalize the corresponding process within the Enterprise Viewpoint as well as the dynamic schema of the Information Viewpoint influenced by that process (e.g., a dynamic schema about the ***Clinical Information*** object would describe the state machine for that object through the version control process).

Finally, the methodology for extensions of HISA is the last point that deserves to be discussed. Although the HISA standard could seem to be imprecise in some respects (as pointed out above), it presents an ability to be extended with more objects and processes, both general and with specific purposes. To do this, HISA defines a set of extension criteria in order to align the developments with its normative core. We consider that these possible extensions, still conforming to the HISA criteria, could be developed without a common normalized background, resulting in systems conforming to the HISA core but with no interoperability between them. Nowadays, there are a lot of standardization efforts covering all the areas of information systems, even applied to the healthcare environment. It is assumed that HISA does not need to standardize the wide spectrum of functionalities of supporting middleware or those related to health-specific purposes. Apart from this, it could be interesting to provide architects with guidelines and references about other standardization initiatives, recommendations, and standards suitable for being used as building blocks for HISA extensions.

In this paper, we have introduced standardization efforts in access control. This extension approach has arisen from a deep revision of initiatives and standards, and harmonization of them when there were divergences. References to SDO could be useful guidelines for architects to extend HISA without abandoning the interoperability approach. Some organizations with wide experience in healthcare information systems, and which could serve as references to HISA extensions, are CEN [7], ISO [8], IHE (Integrating the Healthcare Enterprise) [43], and HITSP (Healthcare Information Technology Standards Panel) [44]. A specific example of an extension related to supporting functionalities could be the adoption of standard interfaces of OMG functions to extend the HISA Computational Viewpoint. In the HISA standard, this viewpoint is quite generic and it does not describe specific interfaces or services. If an architect wishes to formalize functions like the notification service or access control facility, he/she may use interface definitions from the OMG [45][46]. The only risk in this method is the fail to separate platform-independent specifications of features depending on technology, as in the case of OMG, the specifications of which are oriented to CORBA technology. Taking this into account, HISA extensions could enhance the core of this standard based on the experience of internationally well-known SDO.

Furthermore, there are initiatives using the RM-ODP foundations for specifying and managing healthcare service architectures such as SAIF or NEHTA IF. There are some distinctions between these approaches and HISA. For example, SAIF is an architecture conceived to achieve interoperability, but it is not a comprehensive design for enterprise architecture management, and it provides consistency between HL7 artifacts. As remarked in this work, with a precise development, HISA could become a complete architecture in the healthcare environment, independent from particular technological efforts. In addition, NEHTA IF is mainly centered on the actual implementation of eHealth solutions, providing guidelines and interoperability patterns as well as an interoperability mature model to assess solutions, which goes beyond the HISA perspective. In spite of these differences, SAIF and NEHTA IF are useful examples of how to apply RM-ODP foundations to the health domain. They both use the concepts established by RM-ODP, its separation of concerns by means of viewpoints, and even conformance criteria of the framework. Thus, these (and other) contributions must be taken into account in future developments of the HISA standard in order to use semantics provided by RM-ODP more effectively.

5. Conclusions

In this paper, several outcomes from research in healthcare architectural issues have been introduced. This section briefly presents the contributions of these efforts to put architectural procedures in practice. First, the formalization of one of the most relevant efforts to develop normalized architectures applied to healthcare, the HISA standard, has been tackled. Requirements and normative specifications of the HISA standard have been formalized in a way that conforms to RM-ODP, the Enterprise language, and the UML4ODP standard. This implies numerous contributions. The most evident one is that the developed models allow the HISA standard to be easily put into practice by designers and developers, particularly because they have at their disposal the formal representation of the architecture skeleton, and also due to the provision of other mechanisms to make the specification more comprehensible and easily grasped. Moreover, this effort proves that RM-ODP has the necessary semantics to express the multiple issues involved in the formal specification of any distributed healthcare system. In this sense, previous work published by the authors shows how RM-ODP semantics could be expressed in ontology languages (such as OWL) in order to facilitate the introduction of components for semantic management into the architecture [47]. This will improve tasks such as publishing, discovery, invocation, and composition of services in an automatic way, or the effective management of the proactive behaviour of architectural components.

Second, the refinement and extension of HISA with security issues, considering relevant standards as well as HISA procedures and RM-ODP principles, have been exposed. Besides the obvious benefit of introducing formal security models in HISA (reusable by decision-makers, designers and developers), this effort could be considered as a proof of the usability of the HISA formalization developed in the current work, as well as the effectiveness of the HISA extension procedures. The proposed methodology could be carried out to extend HISA in any other relevant topic.

The aim of this research is to facilitate the adoption of architectural procedures for the best management of ICT in the healthcare context. Risks and pitfalls have been identified, as well as some standards suited to be complementary efforts to HISA extensions, all of which are useful inputs for the potential evolution of the HISA standard. The developed tools (i.e., the three technology-independent viewpoints of the HISA-based architecture conforming to RM-ODP and UML4ODP) will be freely available in order to assist healthcare stakeholders in building solutions that realize the benefits of distribution and interoperability via RM-ODP principles. Furthermore, the recent involvement of some members of the research team in international standardization committees could help validate the results and migrate them into official.

Finally, it is necessary to remember our original global objective: to contribute to the effective management of a new generation of services for social, health and well-being care. These services must be built on strong foundations facilitating reuse, interoperability and scalability, in order to take advantage of synergies among them and to offer the optimal scalable and personalized end-services to users. Due to the huge complexity and heterogeneity of healthcare scenarios, advances in normalized healthcare architectures and architectural procedures must be considered as critical instruments supporting this objective. However, it is necessary to understand that much work is required and this line of research is just awakening. Several disciplines, methodologies and computational paradigms will need to be merged in order to arrive at the best framework to achieve the objective, as has been pointed out in this work.

Acknowledgements

This work has been partially supported by the CIBER-BBN, the Biomedical Engineering Group in University of Seville and a grant from the Spanish National Board of Health Research (Fondo de Investigación Sanitaria) inside project PI082023. CIBER-BBN is an initiative funded by the VI National R&D&i Plan 2008-2011, Iniciativa Ingenio 2010, Consolider Program, CIBER Actions and financed by the Instituto de Salud Carlos III with assistance from the European Regional Development Fund.

References

[1] International Standard ISO 12967-1, 2, 3:2009 Health informatics – Service architecture, 2009.

[2] HL7 Group, The Service Aware Interoperability Framework (SAIF), Available on: http://wiki.hl7.org/index.php?title=SAEAF _201001 _Document, Last visited July 2011.

[3] NEHTA Interoperability Framework, version 2.0, August 2007, Available on: http://www.nehta.gov.au/connecting-australia/eHealth-architecture, Last visited July 2011.

[4] K. Kawamoto, A. Honey, K. Rubin, The HL7-OMG Healthcare Services Specification Project: Motivation, Methodology, and Deliverables for Enabling a Semantically Interoperable Service-oriented Architecture for Healthcare, JAMIA 16(6) (2009) 874-881.

[5] International Standard ISO 19793 | ITU-T Recommendation X.906, Information technology – Open Distributed Processing - Use of UML for ODP system specifications, 2008.

[6] International Standard ISO/IEC 10746-1, 2, 3, 4 | ITU-T Recommendations X.901 to 904, Information technology - Open distributed processing - Reference model, 1998.

[7] CEN – European Committee for Standardization, Available on: http://www.cen.eu/, Last visited February 2011.

[8] ISO - International Organization for Standardization, http://www.iso.org/iso/home.html, Last visited February 2011.

[9] OMG - Object Management Group, Available on: http://www.omg.org/, Last visited February 2011.

[10] G.O. Klein, P.A. Sottile, F. Endsleff, Another HISA - the new standard: health informatics - service architecture, Medinfo 12(1) (2007) 478-482.

[11] R. Romero, A. Vallecillo, Formalizing ODP Computational Viewpoint Specifications in Maude, EDOC '04 (2004), ISBN: 0-7695-2214-9.

[12] B. Bordbar, J. Derrick, G. Waters, Using UML to specify QoS constraints in ODP, Comput. Netw. 40(2) (2002) 279-304.

[13] M.W.A. Steen, J. Derrick, ODP enterprise viewpoint specification, Comput. Stand. Inter. 22(3) (2000) 165-189.

[14] MagicDraw UML 16.5 Enterprise Edition. All rights reserved. Copyright 1998-2009 No Magic, Inc.

[15] MagicDraw v15+ plugin for RM-ODP and UML4ODP. Available on: http://www.jrromero.net/tool_mdplugin.html. Last visited February 2011.

[16] ATENEA research group site: http://atenea.lcc.uma.es/index.php/Main_Page. Last visited February 2011.

[17] ISO/IEC 10181-1, 2:1996 Information technology – Open systems interconnection – Security frameworks for open systems, 1996.

[18] ITU-T Rec. X.509 The directory: Public-key and attribute certificate frameworks, 2008.

[19] ITU - Committed to connecting the world, Available on: http://www.itu.int/en/pages/default.aspx, Last visited February 2011.

[20] IETF - Internet Engineering Task Force, Available on: http://www.ietf.org/, Last visited February 2011.

[21] RFC 2828. Internet Security Glossary

[22] RFC 3198. Terminology for Policy-Based Management.

[23] OASIS - Advancing open standards for the global information society, Available on: http://www.oasis-open.org/home/index.php, Last visited February 2011.

[24] OASIS. XACML v2.0 Core: eXtensible Access Control Markup Language Version 2.0. OASIS, 2005, Available on: http://www.oasis-open.org/committees/xacml, Last visited February 2011.

[25] S. Cantor, J. Kemp, R. Philpott, E. Maler, Assertions and protocols for the oasis security assertion markup language (SAML) v2.0. Available on: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, 2005, Last visited February 2011.

[26] ISO/TS 22600-1, 2:2006 Health informatics -- Privilege management and access control, 2006.

[27] J. Calvillo, I. Roman, S. Rivas, L. Roa, Privilege Management Infrastructure for Virtual Organizations in Healthcare Grids, IEEE T. Inf. Technol. B., 15(2010) 316-323.

[28] TANGOS web, Available on: http://gibserv.us.es/wiki/doku.php, Last visited February 2011.

[29] N. Yahiaoui, B. Traverson, N. Levy, A new viewpoint for change management in RM-ODP systems, WODPEC'05 (2005) 1–6.

[30] L. Kutvonen, Using the ODP reference model for enterprise architecture, EDOC'07 (2007).

[31] R. Hilliard, IEEE-Std-1471-2000 Recommended Practice for Architectural Description of Software-Intensive Systems, 2000.

[32] G. Klein, Health Informatics - Service Architecture - The intended role of the EN ISO 12967 standard - An informal guide, 2009.

[33] P.A. Sottile, Approaches in European health information systems architectures, in: Studies in health technology and informatics 96, 2003, pp. 29-37.

[34] I. Román, L.M. Roa, G. Madinabeitia, A. Millán, Introducing guideline management in the healthcare information system architecture, in: Studies in health technology and informatics 127, 2007, pp. 117-124.

[35] T. Senivongse, Y. Teng-amnuay, N. Nupairoj, A Comparison of System Modelling for Distributed Applications: RM- ODP vs MDA, 2004, Available on: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.3440&rep=rep1&type=pdf, Last visited February 2011.

[36] J. Putman, Architecting with RM-ODP, Software architecture series, Prentice Hall, ISBN 0130191167, 2001.

[37] M.P. Gervais, Towards an MDA-oriented methodology, COMPSAC'02 (2002) 265- 270.

[38] International Standard ISO/IEC 15414 | ITU-T Recommendation X.911, Information technology – Open distributed processing – Reference model – Enterprise language, 2006.

[39] B. Traverson, A comparison study of viewpoint approaches in service enterprise architecture, EDOC'08 (2008) 444-451.

[40] J.R. Romero, J.I. Jaén, A. Vallecillo, Realizing correspondences in multi-viewpoint specifications, EDOC'09 (2009) 163-172.

[41] ISO 13235-1, 2: Information technology - Open Distributed Processing - Trading function, 1998.

[42] ISO 14769 - Information technology - Open Distributed Processing - Type Repository Function, 2001.

[43] IHE - Integrating the Healthcare Enterprise, Available on: http://www.ihe.net/, Last visited February 2011.

[44] HITSP - Healthcare Information Technology Standards, Available on: http://www.hitsp.org/, Last visited February 2011.

[45] OMG, Notification Service Version 1.1, Available on: http://www.omg.org/spec/NOT/1.1/PDF, 2004, Last visited February 2011.

[46] OMG, Resource Access Decision Facility Specification Version 1.0, Available on: http://www.omg.org/spec/RAD/1.0/PDF, 2001, Last visited February 2011.

[47] I. Román, L.M. Roa, G. Madinabeitia, L.J. Reina, A Standard Ontology for the Semantic Integration of Components in Healthcare Organizations, in: L. Bos et al. (Eds.), Medical and Care Compunetics 3, pp. 257-265, ISBN: 1-58603-620-3.

There are no biographies or photographs of authors in time of submission