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).
1386-5056/$ – see front matter
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 his/her health resources in a user-friendly and flexible way and deep granularity. The access control infrastructure shown in this paper is based on two essential points differentiating it from other studies. Firstly, it is completely oriented to be part of a standardized Healthcare Services Architecture following the SOA paradigm (Healthcare SOA, HSOA). To achieve this, the requirements of standards and methods for design and development (conforming to security standards [15–21], formalization in viewpoints [22–24], etc.) are taken into account. The second point relates to the usability of solutions to ease the administration tasks to the SoC. For this specific purpose, we introduce the Me-As-An-Admin (M3A) application, which guides the SoC through the specification of personal access policies to his/her distributed resources by using semantic technologies.

1.1. *The Person-Oriented Virtual Organization paradigm*

At a high level, the SoC-centric paradigm covers a set of resources (human, administrative, computational, and informational) belonging to different administrative/technological domains, which are often geographically separated. In addition, resources are subject to sharing rules defined by an administrator who, in this case, is the very SoC to whom resources refer. This definition shares some features with the VO concept originally developed within the business domain and later adopted by the distributed system architectures [25,26]. By definition, a VO is formed in order to accomplish an objective common to all the stakeholders. In the healthcare domain, this objective would be the health, well-being and social care of a particular SoC (who is the administrator of the VO). To emphasize this orientation toward an SoC, we propose a new concept focused specifically on this domain: the Person-Oriented Virtual Organization (POVO). Both the VO and POVO integrate heterogeneous systems distributed across administrative boundaries, and the different spanned domains must define cooperation links between them. An important divergence between these approaches is that the security in a VO is shared among the administrators of the involved domains. On the contrary, in a POVO, the correspondent citizen is the exclusive administrator of the resources and he/she can decide over who has access to them. Furthermore, while a VO is dynamically created to complete a business process, a POVO is strongly linked to the healthcare process performed during a particular person's entire life. Thereby, a unique POVO is created for each individual, evolves when his/her desires change, and is only destroyed when his/her life comes to end.

The purpose of using the term "person" (e.g., instead of "patient") is to emphasize that the POVO scenario centers on SoCs who are not only patients in treatment or monitoring but also any healthy individual involved in prevention tasks following the continuity of the healthcare model. Thus, healthy citizens can, for example, manage resources promoting their healthy life habits (meal ingestions, exercises performed, etc.), maintain their well-being, prevent against diseases which they are prone to for genetic disposition, and so on.

The complex model approached behind the POVO concept entails new requirements and scenarios to study. Since this paper focuses on the access control mechanism as an essential building block of POVO, we identify the requirements specific for this issue (instead of those for the whole POVO scenario):

- The POVO paradigm is SoC-centered, thus there shall be a unique POVO instance for each SoC. This instance shall cover all the resources related to the SoC during his/her entire life without the need for managing (i.e., creating/destroying) multiple instances. Nevertheless, an instance shall evolve anytime to meet the SoC's desires.
- The SoC is the owner of all the information related to his/her health and he/she must have absolute authority over access to that information within his/her POVO. Besides, the SoC must only be able to control access to the resources available in his/her POVO when those resources use information about him/her (see next point).
- Since resources shall be deployed and maintained by healthcare organizations or third parties, they will be subject to access (and use) policies defined by their legitimate owners. If resources use information related to the SoC (e.g., a computational model from an insurance company that is fed with health data), these policies cannot interfere with those specified by the SoC to control the access to the resources within his/her POVO (i.e., involving information related to his/her health).
- Access control policies must be as flexible as possible and allow different granularity levels covering the broadest range of the SoC's wishes and preferences.
- The SoC must be able to create, modify, and delete his/her access control policies.
- Both the management interface and the involved terminologies must ease the interaction of the end-user and promote usability. Administration tasks must be as seamless as possible in order to allow the SoC to exploit the management capabilities of his/her POVO without need for advanced knowledge.
- There must be mechanisms of delegation of management privileges in order to cover scenarios where an SoC has no desire to manage his/her resources. Moreover, these mechanisms must be flexible enough to support the administration by parents or legal guardians in case of infants or disabled people.
- Regional legislation and international directives establish scenarios where the SoC's authority over his/her resources can be temporally invalidated [3–7]. Therefore, accessing a resource without the SoC's consent and violating existing policies must be possible if, for example, a health hazard or an emergency exist, with which delays can result in irreversible injuries or death risk.
- There must be auditing mechanisms to allow the recording of activities by users in a chronological order. All the information about access attempts (either successful or not), use, or modification of resources must be recorded.

The supporting access control infrastructure for the POVO has been designed according to these access control requirements. The access control infrastructure is the first building block of the POVO, which is composed of a wide spectrum of services. Looking at the big picture, a personalized and comprehensive health, social and well-being care could be supported by the combination of heterogeneous useful services. Value added services can be created in an easier manner, by combining previously existing capabilities, only if services are provided by systems designed by considering reuse and scalability. In this sense, we are designing an HSOA in which we combine and extend international standards for healthcare information services architectures [23] and others for specific fields such as security [15–21,27]. Details of the infrastructure and HSOA have been developed in a previous paper [28] and here we focus on issues of policy specification by the SoC. In the next section, the background of this paper is presented by identifying the main tools and technologies used.

2. Background

2.1. *Architectural Issues*

The POVO paradigm is supported by a healthcare architecture based on SOA and standards, improving interoperability, reuse of capabilities, and integration. An effective integration and composition of services supporting advanced capabilities can only be achieved through the deep understanding of the overall architecture. Furthermore, a precise formalization (e.g., based on modeling) of the healthcare architecture supports reasoning about the structural properties of the system and eases its evolution and the addition of new elements and services. A formal specification defines system components, or building blocks, their relationships and provides a plan from which products can be procured and systems developed.

The suitable design and formalization of such an architecture must be done by using tools (i.e., frameworks, methods, and formal languages) from existing standardization efforts. Architectures adopting standards can aspire to acquire greater acceptance due to follow guidelines developed in consensus with Standard Development Organizations (SDOs). Different standards provide frameworks and reference models for the formalization of distributed system architectures. Two examples are the Reference Model-Open Distributed Processing (RM-ODP) [22] and the Model Driven Architecture (MDA) [29]. Although these standards differ in many aspects (e.g., viewpoints in ODP against a model approach in MDA), they do have a similar philosophy. They separate specifications targeting a technology-neutral viewpoint of the system (Platform Independent Model, PIM) from those including details that specify how a particular underlying technology is used in the system (Platform Specific Model, PSM). Since a particular PIM can be translated to different technological platforms, this approach improves the interoperability between components designed by following the same PIM even though they may have been developed using different technologies. Furthermore, this principle also facilitates the evolution of system components supporting the lifecycle and the migration of hardware and/or software and allowing the reuse of assets.

The RM-ODP has been chosen for the standardization of healthcare services architectures in the European standard EN12967 (Health Informatics Services Architecture, HISA) [23] accepted as an ISO (International Organization for Standardization) standard in 2009. It is pointed out that the ISO/EN 12967 does not aim to represent a final complete set of specifications. On the contrary, it only formalizes features that are common and currently essential in any advanced healthcare system, as well as relevant for any healthcare sector. Therefore the ISO/EN 12967 standard is an open framework that can be extended during time according to the evolution of the healthcare organization. Specifications are formalized avoiding any dependency on specific technological products and solutions.

2.2. *Access control policies*

Security has been the focus of much effort due to the wide range of separate services (i.e., authentication, authorization, privacy, trust, etc.) that it covers. Several SDOs have proposed security frameworks in order to define common concepts and requirements related to security issues. Due to its particular relevance for this paper, we focus exclusively on access control. However, other security issues will be addressed in future efforts. Access control has motivated several approaches such as the Role-based Access Control (RBAC) [30] or the Attribute-Based Access Control (ABAC) [27]. The RBAC model is particularly interesting since organizational roles can be assigned to subjects, and access privileges are related to roles instead of directly to subjects, easing management tasks and scalability. In addition, in the ABAC schema, a role can be any attribute of the subject such as the professional category or the place of residence (i.e., roles are not restricted to organizational positions like in the RBAC).

The approaches supporting distributed and federated access control reclaim methods and languages for policy specification. Two of the most relevant initiatives are the standards eXtensible Access Control Markup Language (XACML) [15] and Security Assertion Markup Language (SAML) [16] published by the Organization for the Advancement of Structured Information Standards (OASIS). XACML is a general purpose, flexible, and powerful language for specifying and enforcing access control rules following the ABAC model. SAML is a language for interchanging information relative to security assertions, also defining a communication protocol.

Meanwhile, the healthcare domain has its own approaches and recommendations on security. In particular, the Technical Specification ISO 22600 [17] is intended to support the needs for healthcare information sharing across unaffiliated providers, organizations, insurance companies, SoCs and so on. This supports the collaboration among authorization managers that may operate over organizational and policy borders. Moreover, it introduces the underlying paradigm of formal high level models for architectural components based on RM-ODP. Besides that, there exist standardized profiles for using XACML and SAML in the healthcare domain published by OASIS [18,19]. Furthermore, some initiatives aim at establishing guidelines and service specifications related to access control. Efforts such as Integrating the Healthcare Enterprise (IHE) [20] and Healthcare Information Technology Standards Panel (HITSP) [21] must be taken into account.

2.3. Tools and technologies for domain knowledge specification

2.3.1. Semantic technologies and access control

During the last decade, semantic technologies have been developed enormously because of the benefits, which they provide to distributed systems. One of the most popular semantic tools is the Web Ontology Language (OWL) [31]; a knowledge representation language based on description logic and the Resource Description Framework (RDF) representation. OWL allows the specification of domain knowledge by using classes in ontologies. Reasoners or inference engines work over instances of these classes, and this process allows inferring implicit information about the instances according to the domain ontology. Although simple inferences can be realized on OWL, a limitation in the reasoning process exists because OWL does not allow using more complex rules than the inheritance of classes. A special rule language is required in order to write rules composed of OWL concepts and to reason over ontology instances. A promising approach is the Semantic Web Rule Language (SWRL) [32], which allows establishing complex relations among properties by extending the OWL expressivity. SWRL supports the construction of "Horn-like" rules expressed over OWL concepts.

There are current efforts applying OWL in the formalization of access control policies [33–35] in conjunction with SWRL [36,37]. Three main advantages can be obtained from the use of ontologies to describe resources and inference engines for reasoning. First, SOA characteristics such as openness and interoperability are enhanced since the understanding between different parties is eased. This is achieved by sharing the formal definitions of resource descriptors as ontologies. The administrator will use these concepts to label the resources of his/her POVO. Second, by passing an ontology of concepts through a reasoner, new knowledge about the resources can be inferred and it could be added as explicit relations and elements. Lastly, by introducing semantic inference in the access control mechanisms, the development of decision making elements can be eased. Access control policies would be expressed according to ontologies (i.e., resources, user attributes, environment, etc.) and rule languages. Thus, the logic of decision points could be reduced to an inference engine, the result of which would be the access permission or prohibition.

The introduction of ontologies and semantic tools in an SOA can be addressed from very different viewpoints as previous papers have shown. For example, some authors have modified the XACML framework to accommodate semantic elements [37–39], which allows performing inference phases over attributes or policies. Other schemas include semantics in access control models [40,41].

2.3.2. Domain specific languages (DSLs)

DSLs constitute an increasingly more popular area within the Model-Driven Engineering (MDE) community because of their simplicity compared to general-purpose languages and their focus on the domain of interest. A DSL is based on a metamodel (the abstract syntax specifying the concepts of the language and their relationships) and a specific syntax (allowing users to create models conforming to the metamodel). Among the available tools supporting the development of DSLs, the Eclipse Modeling Framework (EMF) is one of the most promising [42,43]. To alleviate some weaknesses in terms of required effort for development, some plug-ins have been created supporting advanced functionality and making some low-level tasks transparent. These are the Graphical Modeling Framework (GMF) [44] and EuGENia [45].

The MDE philosophy proposes to work with models in a certain level of complexity and then transform them in others models of different levels. But besides the transformation between models, there also exist tools to transform from model to text such as MoFScript [46] or the Model-to-Text (M2T) initiative [47]. These are based on a file where transformations are specified by using templates, indicating to which piece of code or text each model element corresponds.

There have been a lot of efforts related to DSLs to access control [48,49], but only a few have focused on the healthcare domain. A remarkable solution was SPARCLE [50], a privacy policy workbench supporting individuals to define policies using natural language.

3. Results

The results of this paper are supported by the background described above. The relations among the POVO paradigm and the tools and methods are presented in Fig. 1. Firstly, the POVO paradigm is supported by a SOA fulfilling the requirements of HISA and RM-ODP. A contribution of this paper is the extension of the HISA foundations with access control features not covered by this standard (Section 3.1). With regard to ODP viewpoints, a great effort has been made in order to develop the PIM as detailed as possible. Furthermore, it intends to serve researchers and developers as a very open framework that allows them to use any particular platform and to deploy services and devices in the most suitable manner for particular scenarios.

The approached authorization schema for the POVO follows the ABAC guidelines. The SoC establishes correspondent privileges by means of policy definition. We use the OWL language to develop an ontology of resource descriptors, involved actors, and context characteristics that could be implicated in the access decision (such as the physical location where the access is performed from, date and time, etc.). The potential attributes for users are specified in the POVO ontology and, in any case, they will refer to the relationship that each individual has with the SoC. This feature solves the problem of implementing RBAC models in multi-organizational scenarios with separate administrative boundaries where roles are related to hierarchy inside the different organizations. Thus, in the proposed approach we use the relationship of users with the SoC which allows having roles independent of administrative hierarchies; and it perfectly matches the SoC-centric approach.

Access control policies will be expressed by using SWRL rules. We have chosen Jess [51] as the inference engine due to its compatibility with Protégé-OWL platform [52], which allowed developing the knowledge base, i.e., OWL ontology and SWRL rules. These tools are used to build an access control mechanism for the POVO, although our approach emphasizes

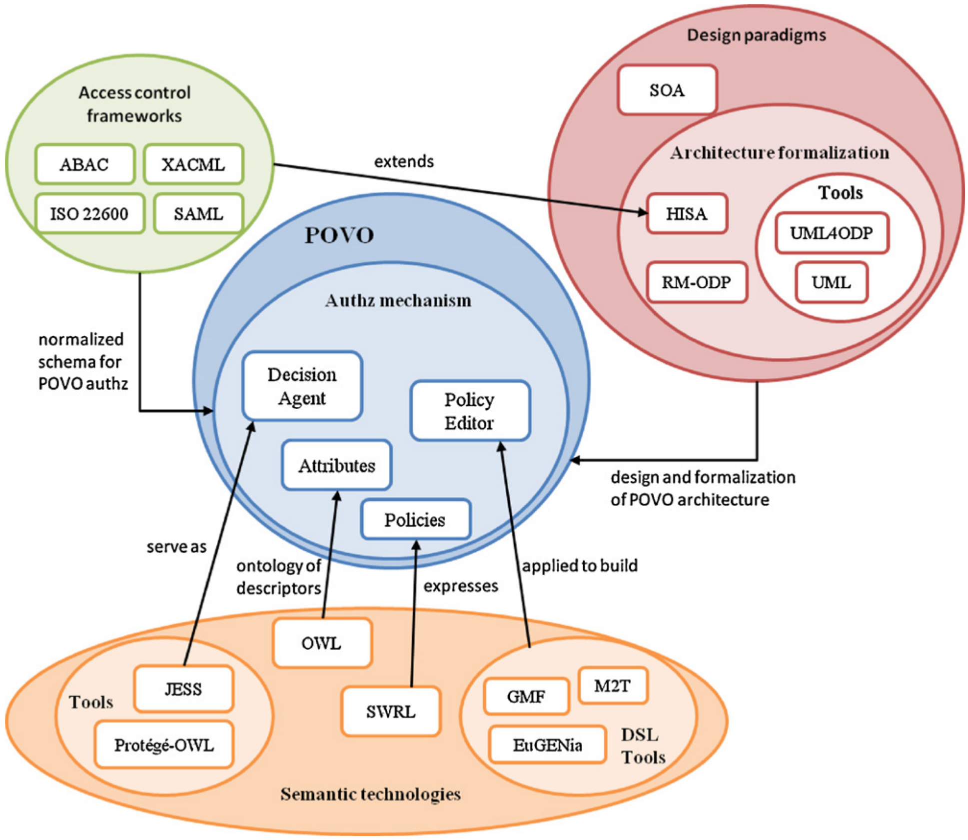

Fig. 1 – Schema of relations of tools and methods and the POVO paradigm.

their independence of specific technologies. Finally, a meta-model and its correspondent editor have been built by using the GMF and EuGENia frameworks from the POVO ontology in OWL. As is described below, an SoC is assisted to create models of his/her preferences of access control to his/her resources. These models are automatically transformed to text (specifically to SWRL rules) using M2T and included in the knowledge base composed of the POVO ontology and SWRL rules. The knowledge base is the Policy Information Point (PIP) supporting the decision making of the Policy Decision Point (PDP). The whole process is extensively described in Section 3.2.

3.1. *Architectural design*

Although this paper mainly focuses on policy editing and access control decision making, the developed security elements are basic building blocks of the POVO scenario, a complex and evolving paradigm supported by distributed systems compliant with a standardized architecture. The access control tools shown in Section 3.2 are an example of mechanisms contributing to a shift in the health delivery process, making it possible for the SoC to be the administrator of his/her health resources.

RM-ODP and HISA have been chosen for the standardization of the healthcare service architecture supporting our approach. The HISA standard only formalizes fundamental aspects, which are common and currently essential in any advanced healthcare system, hence it has been extended with different features.

Standardized access control concepts and objects have been integrated into HISA whenever they were not explicitly stated in this standard. Fig. 2 shows an information model as an example of the Information Viewpoint according to Rec. X.906 [24]. The model corresponds to a static view of the information objects of the user and authorization management activities specified by HISA. To this set of objects (identified as 'i' circles following the X.906 norm), we have added those related to security (drawn as boxes) such as *Access control decision* or *Attribute*. HISA information objects not directly linked to our approach have been hidden for the sake of clarity. Some examples of integration relations between HISA and the security extension are: an *Authorization profile* will be composed of, at least, an *Access control policy* and managed by a *Policy information system;* an *Access control decision* is made by a *Policy decision system* and links a *User* and a *Controlled element.*

Moreover, the integration of the HISA Computational Viewpoint (third part of [23]) with the POVO objects is performed by establishing one computational object for each information object related to security. In order to include computational objects of access control, the requirements of the HISA Computational Viewpoint must be taken into account. The systems involved in the access control processes are defined here as computational objects and their methods are 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 not separate completely the applied recommendations (e.g., XACML) from specific technologies (e.g., XML), which must be

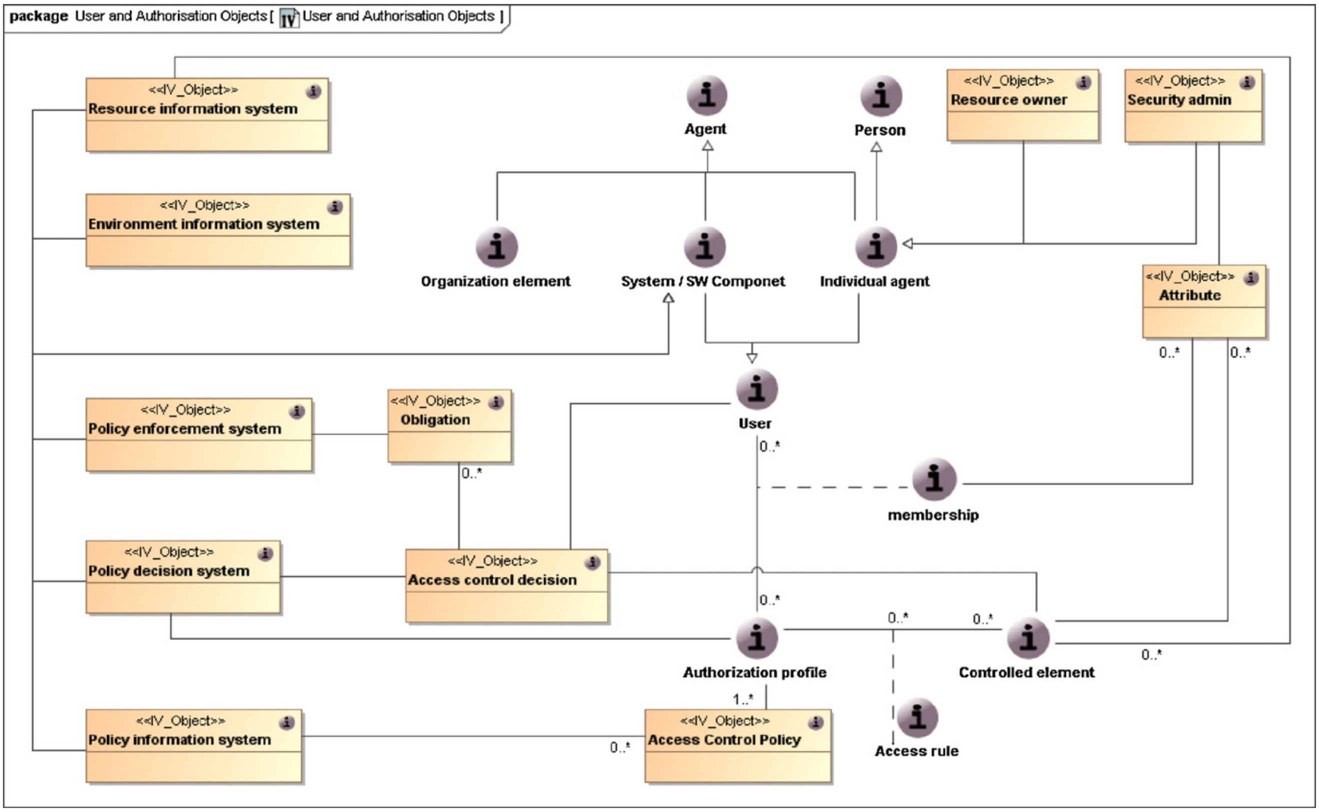

Fig. 2 – Model from the Information Viewpoint integrating HISA with access control objects.

specified in the Engineering and Technology Viewpoints, but not here.

Finally, it must be emphasized that the components supporting the access control in our approach have all been designed as services inside the HSOA, by using X.906 for their inclusion and formalization in the different ODP viewpoints, improving their reutilization and scalability.

3.2. Translating the preferences of the SoC to machine-processable rules

An essential requirement to make the management by any SoC of his/her POVO feasible is to emphasize the importance of usability and transparency of low-level details. Among the administration tasks, the SoC must be able to define access policies in different granularity levels. An example of a coarse-grain policy is "to allow the access to the resources of my POVO to any healthcare professional". On the other hand, a fine-grain policy could be "to allow my partner to see all my information related to sexually transmitted diseases since year 2000 and in which third persons are not involved".

Our approach to translate these preferences (i.e., access control policies) to machine-processable rules is illustrated in Fig. 3 and detailed below. According to [15], the PIP and the Policy Administration Point (PAP) perform tasks of policy provision and administration, respectively. The PDP makes decisions, and the Policy Enforcement Point (PEP) intercepts accesses. The Context Handler and other elements have been excluded for sake of clarity (a view of the complete architecture is detailed in [15] or [41]).

3.2.1. POVO ontology and metamodel

To achieve the degree of flexibility required by access control policies, an ontology has been modeled for the POVO fulfilling all the potential features of resource categorization in the healthcare domain. By using this ontology, the SoC can have a versatile control over the access to his/her resources through: the potential actors who can access them, the nature of the information or the diseases related to him/her, creation dates, authors, physical location of access, etc. The developed ontology first appeared in [28] but it was described only briefly.

This ontology covers basic concepts in a POVO and is composed of three parts: an ontology of healthcare actors, another focused on resource descriptors, and a third describing security issues to create access control policies. We have used the terminology of the European standard EN13940 [53] as the basis for the definition of numerous concepts and we have considered others with the purpose of meeting the great variability that currently exists. In addition, a multilingual labeling of concepts through RDF capabilities has been performed allowing non-English speakers to use the ontology.

The ontology of healthcare actors identifies three main groups: people, organizations, and healthcare devices. The people group includes real individuals ranging from the SoCs themselves and healthcare professionals (physicians, nurses, etc.) to SoC's relatives, friends, and caregivers. A potential

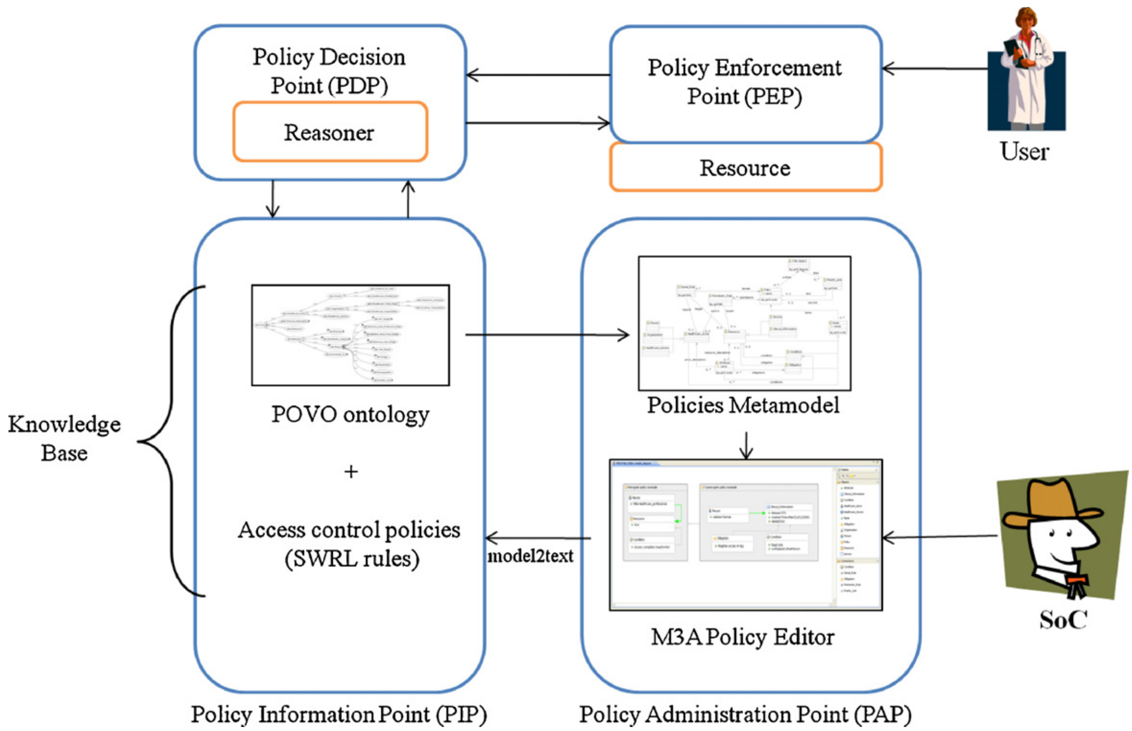

Fig. 3 – Relations between the elements of policy edition and access control decision making.

attribute for describing individuals identifies their relationships with the SoC (e.g., CHILD, PRIMARY, FRIEND, etc.) and this feature, among others, is used to feed the access control mechanism. The SoC will also be able to create new relationships fitting his/her needs. The second group of actors is related to organizations including both medical (hospitals, departments, clinics, pharmacies, etc.) and other institutions that may play a role in the healthcare delivery process of the SoC (e.g., those involved in the maintenance of health and well-being such as gyms or dietary centers, insurance companies, laboratories or independent research groups, entities that deploy and maintain healthcare resources, etc.). Finally, the third group includes the healthcare devices that have an important role in the healthcare environment as sources or sinks of information. They even sometimes work on behalf of real people, either healthcare professionals or the SoC.

Two groups of objects to which access must be controlled have been considered: information and other resources. Both groups have attributes to be identified as well as control of versions and auditing. Information is structured into elements covering all the features related to health such as results of diagnostic tests, medications, exercise routines, eating habits, genomic information, etc. Resources (e.g., databases, simulation and modeling software tools, etc.) are deployed and maintained by organizations and manage pieces of information about the SoC.

Both information and resources will be categorized by using descriptors that allow pointing their nature (e.g., demographic, healthy lifestyle, eating habits, diseases, etc.) and indicating whether they are anonymized or not. Besides this classification (that can be done more or less automated), we have included other descriptors to ease the access policy creation. Thus, an SoC can, for instance: determine which information is available for navigation and which is exclusively for his/her assistance; establish a control schema based on confidentiality levels; indicate what drugs, diagnostics, and treatments belong to his/her past health record and have no impact on the present; and a wide range of possibilities.

In addition to the described features of the ontology, others are introduced focused on the relationship of the SoC with organizations (contacts, meetings, events and periods of attendance, etc.), on the classification of activities considering who executes them (automated by devices or performed by caregivers, health professionals, or the SoC him/herself), and on the access policy formalization (discussed in the next section). It must finally be clarified that the developed ontology does not try to build a complete solution but only represents basic concepts of a POVO illustrating how the access control could be solved in the presented scenario. Nevertheless, it is a flexible and scalable solution that can, through mechanisms for importing and merging ontologies, be fed on other widely accepted initiatives (for example, [54,55]).

A metamodel for the access control policy editor has been built from the POVO ontology. Due to the wide range of concepts that the ontology holds, and for simplicity, we have worked on a reduced version holding only the security ontology (essential for the access control policy editing) and the healthcare actor ontology. The metamodel has been created in Emfatic [56], a convenient textual syntax for Ecore, and Fig. 4 shows the main concepts and relationships. This metamodel serves as a proof of concept for showing the usability of a solution oriented to SoCs. In a real scenario, it should be extended

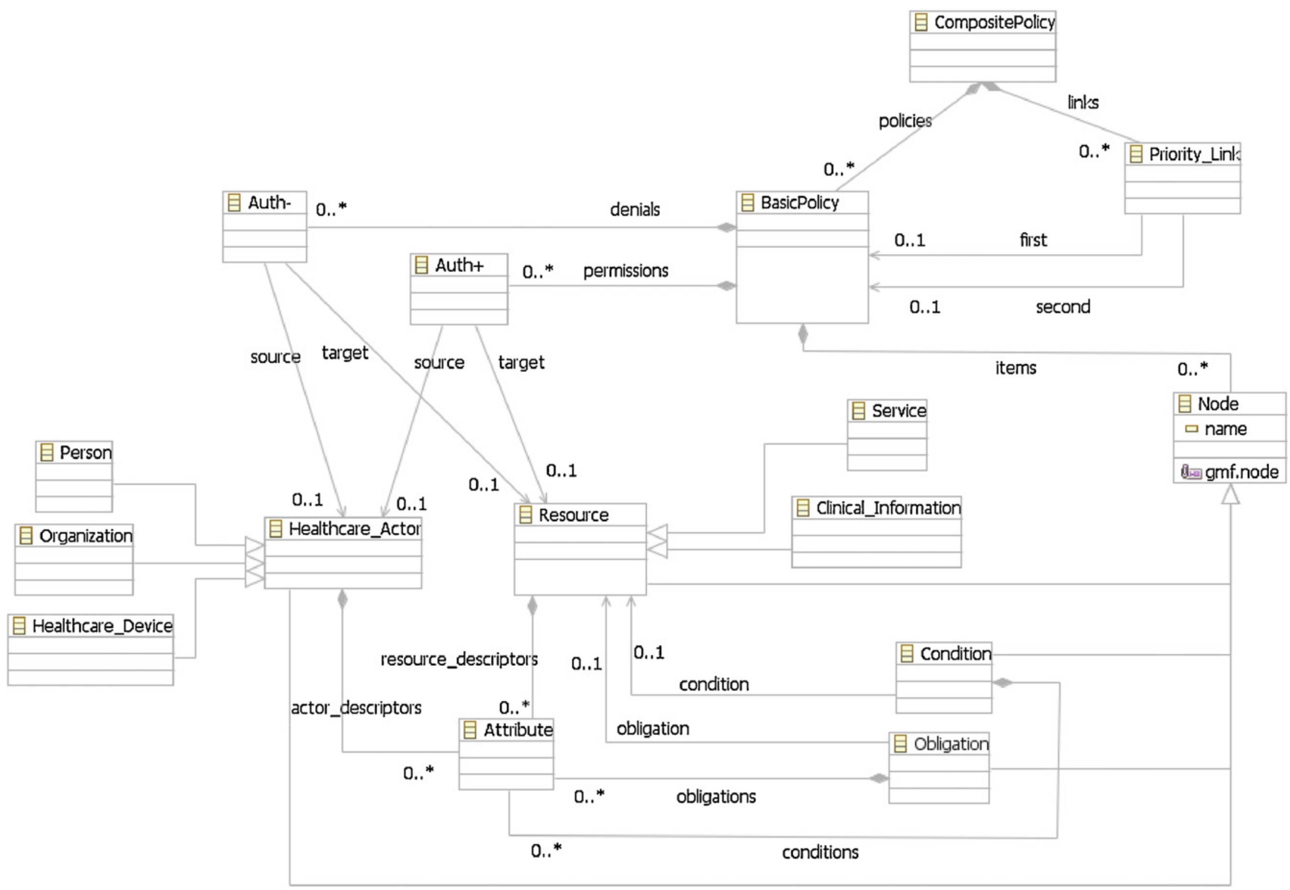

Fig. 4 – Simplified metamodel for the access control policy editor.

with the whole POVO ontology and related standards. In this simplified metamodel, we introduce some concepts from ISO 22600 (*BasicPolicy*, *CompositePolicy*, and so on) illustrating a starting point of the integration with this standard.

As is depicted in Fig. 4, the main concept is *BasicPolicy* which contains *Nodes* and *Links*. Nodes are used for policy edition and include: *Healthcare_Actor* who requests the access, *Resource* being accessed, and *Obligations* and *Conditions* that limit and impose restrictions to the access. Each node may hold *Attributes* which are textual in this first version. The relation between an actor and a resource is established through *Auth+* or *Auth−*, specifying whether the access is permitted or denied a priori (i.e., conditions will have to be satisfied for granting access). Moreover, a *Priority* relation between policies can determine a preference in the checking order. This simplified metamodel has allowed building the M3A editor by using EuGENia tools.

3.2.2. *Me-As-An-Admin (M3A) – a user-friendly access control policy editor for empowered citizens in health*

Usability has been identified as a major asset to transfer the results of security and privacy research to practice in real systems. There has been limited research into how to make complex security and privacy functionality understandable to those who must use it. This condition is essential in the POVO paradigm because the administration is carried out by the SoC, who maybe unfamiliar with technology. Thus, M3A is designed to support SoCs with a variety of skills. The policy definition is made by using models that will automatically be transformed to the machine-readable policy, i.e., as SWRL rules. Fig. 5 shows a screenshot of the M3A editor.

The editor includes a palette with the elements defined in the metamodel, and the SoC only has to drag and drop them into the workspace. Fig. 5 shows an example composed of two policies. The left policy specifies the coarse-grain rule of Section 3.2 (i.e., any healthcare professional can access any resource for reading and writing with no restrictions or conditions). The right one describes the fine-grain policy indicating that the SoC's partner can read his/her clinical information related to sexually transmitted diseases (STDs), which has been created after 01/01/2000. A condition limits the partner from reading information identifying any other person than the SoC. Furthermore, it is obligated that the access must be registered in an event log if it is to become successful. In this example a priority exists between the coarse-grain and the fine-grain policies. The latter must always be satisfied in first instance, therefore even though the SoC's partner were a healthcare professional, he/she could not read clinical information related to STD between the SoC and his/her former partner (even after year 2000).

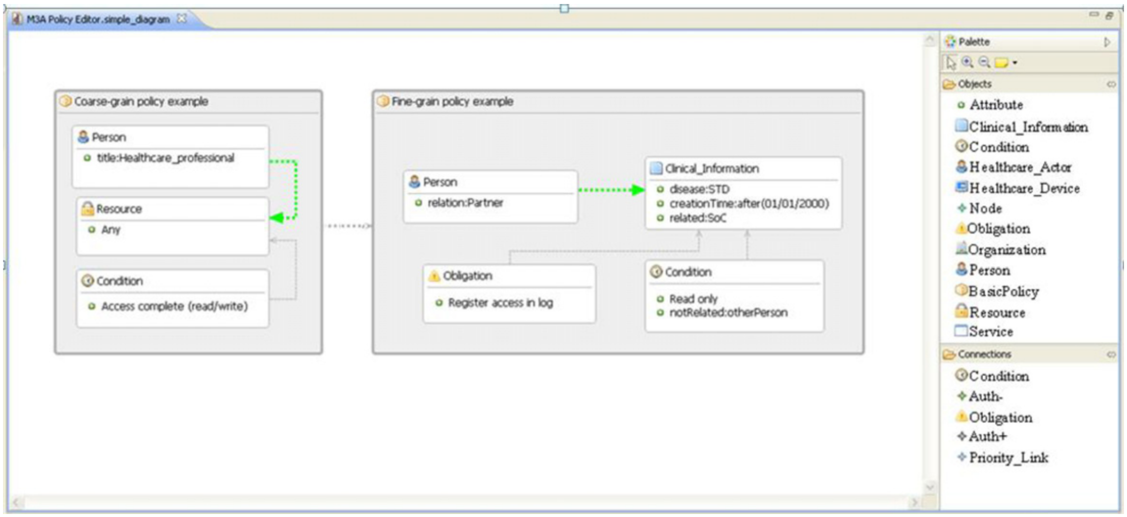

Fig. 5 – M3A policy editor and two example policies.

In order to evaluate the usability of the M3A editor, a first validation phase has been performed on users with and without technologically skills. The acceptance has been generally high from both groups, and the most valued feature has been the intuitive interface. The usage results have allowed defining several restrictions in order to reduce common mistakes that may lead to malfunction. Some of these restrictions are: a priority link cannot be established between a policy and itself, there may only be a relation between an actor and a resource, policies cannot be unnamed, etc. These restrictions have been specified through the Epsilon Validation Language (EVL) [57], a language similar to the Object Constraint Language (OCL). The special contribution of this approach is to assist SoCs with various skills to manage the access control to his/her POVO resources, thus a further validation is in progress with a large group of individuals and questionnaires to evaluate their experiences. The results of that validation phase will be more valuable to enhance the editor usability.

The last, but not least, point of the procedure consists of transformations from model to text. Transformation rules have been defined by using the M2T project tools, which allows obtaining from the metamodel instances created by an SoC, a plain text file with the corresponding policies as SWRL rules. These policies are incorporated into the POVO knowledge base (Fig. 3) for the subsequent query by the PDP. The rationale and description of the access control policies proposed in this paper are extensively described in the next section.

3.2.3. *Access control policies*

Access control policies are stored in the knowledge base as SWRL rules. In this approach, a policy is a “Horn-like” rule in which the antecedent is composed of elements (actors, resources, attributes, environment features, etc.) conditioning the decision, and the consequent specifies whether the requested action is permitted or prohibited. The specification of the two examples shown in Section 3.2 (which illustrate policies of coarse and fine-grain) as SWRL rules is:

who:Healthcare_Professional (?p) ^ what:Clinical_Information(?i) → **actionPermitted**(?p,?i)

who:Person(?per) ^ who:hasRelation(?per, who:SPOUSE) ^ what:Clinical_Information(?inf) ^ attr:Sexual_Organs(?dis) ^ isRelatedTo(?inf,?dis) ^ attr:Subject_Of_Care(?soc) ^ isRelatedTo(?inf,?soc) ^ what:creationTime(?inf,?time) ^ temporal: notBefore(?time, “2000-1-1”) → **actionPermitted** (?per,?inf)

The interpretation of a rule like the previous one is: if conditions specified in the antecedent are true (i.e., there are OWL instances satisfying all clauses), then the property ‘actionPermitted’ must be created among actor/s and resource/s. Although these two examples are permissions, prohibitions follow the same schema with ‘actionProhibited’ instead of ‘actionPermitted’ in the consequent. The process of rule checking and properties creation will be realized by an inference engine as is explained below. Jess has been used in this technological resolution, but the approach is technology-independent and it could use any engine.

Before that, we must clarify how different policy ownerships coexist in a POVO. Three entities are able of creating access control policies: the SoC who owns authority over his/her information and can define rules according to his/her wishes, providers of the resources involved in the POVO who control access to them but who cannot interfere with policies defined by the SoC over his/her information, and finally, regional and international legislative organizations specifying policies to apply in exceptional scenarios in which the SoC’s authority can be avoided. The access control specifications imposed by these three groups must coexist, and incoherencies cannot appear since they would result in incorrect decisions being made. Our solution is based on the following points:

- The policies established by legislative organizations have the highest priority level. Thus, a decision made in accordance with a policy of this group automatically overturns any policy stated by the SoC or resource owners. Among the legislative policies we can find, for example: those permitting the SoC to access all his/her information, or those considering emergency scenarios (physical injuries or death to SoCs, notifiable diseases, or health hazards). Although this policy group will always be activated, it only rules exceptional cases. In the usual execution of the system, the SoC's authority will seldomly be overturned.
- In a common scenario with no emergencies (i.e., no legal policies triggered), the policies defined by the SoC are responsible for the access control. The examples shown above illustrate the kind of policies included in this group.
- The third group is composed of the policies established by resource owners. These can only regulate the access to resources and never to information about SoCs. Since in general the resources will manage information to perform their tasks, a policy ruling the access to a resource must take into account the policies defined by the SoC for the piece of information used. Thereby, it can happen that a user has access to a resource (because the policies of the corresponding owner permit it) but not to the information used by that resource (as this is what the SoC specifies). The opposite case is also possible, a user can have access to clinical information but not to the resource using it (e.g., applications for statistical reports).

The decision making process performed by the PDP follows the schema shown in Fig. 6. When a PDP receives all the required information, firstly it combines the POVO ontology with the SWRL rules corresponding to the legal group, and the inference engine executes the inference. The inferred axioms are incorporated into the ontology, and a query language (in this case, the Semantic Query-Enhanced Web Rule Language, SQWRL) is used to verify the existence of the 'actionPermitted' property between the access requester and the requested resource. If the legal policies have specified this property, then access is permitted. In another case, a new query is performed by searching for the 'actionProhibited' property and, if it exists, the requester is denied access. In case no decision being able to be made, the inference process is once more executed but now with all the rules, i.e., adding the policies defined by the SoC and those by the resource owners. Once again, two queries are created to verify the existence of the properties of permission and/or prohibition. In this point, the possible scenarios are:

1. There is a property of permission (or prohibition). Then the decision of access acceptance (denegation) is made.
2. Two or more policies defined by the SoC are incoherent, and the two properties (permission and prohibition) exist at the same time. In this case, the most conservative decision is made (i.e., denying the access).
3. There is no policy ruling the requested access and, since language is based on what is known as the open world assumption (OWA) (explanation described in the next paragraph), no decision can be made. This scenario is solved by making the PDP deny the request.

The reasoning process over OWL is based on the OWA establishing that if something does not exist, it cannot be supposed. This notably affects the decision making in the POVO because there will always be access attempts not covered by policies. According to the OWA, in these cases, it cannot be supposed that access is prohibited. Thus, previously it will have to make a decision to cover cases without policy. We will make the most conservative decision consisting in denying access to the attempts not covered by POVO policies. In addition, all attempts will be registered by following log and auditing principles. Uncommon scenarios will be argued in the next section.

4. Discussion

4.1. *Exceptional scenarios of SoC administration*

In the previous sections we have covered the access control features required by the POVO paradigm and considered the common functional scenarios of access control. Besides these, there are complex questions that must be analyzed and solved. They are discussed below, and the rationale of how technology could support them is also presented. Despite this, it is out of the scope of the present paper to give a particular solution to each one.

The first scenario we must analyze is in that the SoC is an infant. In the general situation the mechanisms of delegation of administration rights allow, if the SoC desires or he/she is legally disabled, granting the privileges of his/her POVO management to another person or administrative entity. Since that moment, the delegate obtains the role of POVO administrator and is able to access the information and resources, and create, modify and delete policies as if he/she were the SoC. Nevertheless, the SoC maintains his/her rights and can continue using them. The case of infants poses higher complications because unlike the previous situation, it is not permanent. Now the scenario suffers an evolution. First the POVO management is performed by the parents or legal guardians, and the infant cannot access his/her information or resources. When the infant reaches legal age, he/she becomes responsible for the administration of his/her POVO, and parents and guardians lose their privileges. This process can even happen gradually (according to related legislation) and the more the infant grows, the more privileges he/she receives to manage the features of his/her health information, usually starting with the less sensitive elements. The policy specification in our approach allows establishing limits in access to information to each individual (the SoC and the guardian) during this process. This only leaves the question of how the privileges for policy management pass from guardian to infant when he/she reaches legal age to be resolved.

The second scenario that deserves consideration is that in which various POVOs coexist. From the definition of the concept (and always according to applicable legislation in each country), the SoC is the owner of all the information related to his/her health and, within his/her POVO, he/she has absolute

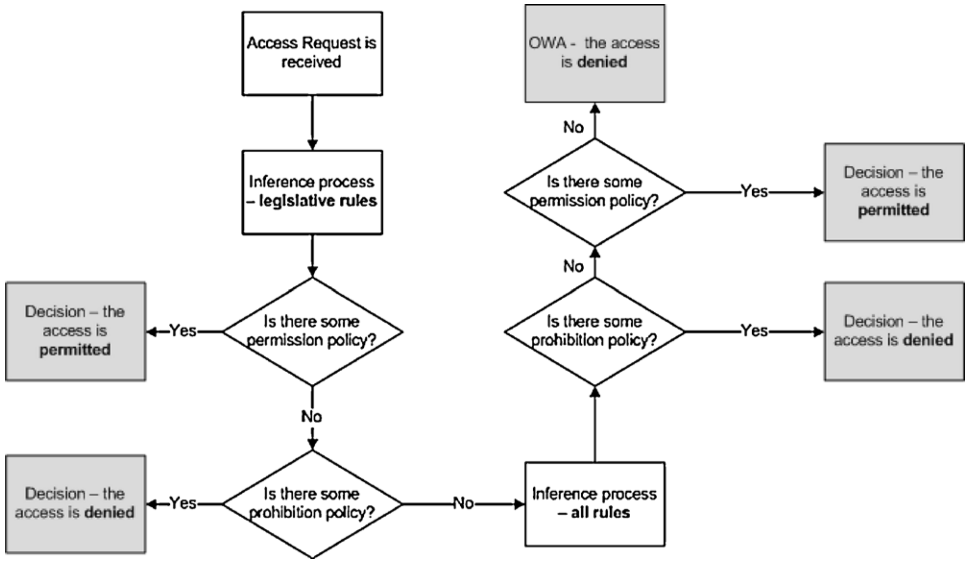

Fig. 6 – Access control decision process based on rules within the POVO scenario.

authority over the access to the resources containing or using that information. Thus, access to information of any nature can be restricted to the individuals whom he/she desires. The problem arises when access to a certain piece of information is denied to an individual involved in it. For example, a father with a hereditary disease establishes policies prohibiting the access to that piece of information to his children. Then, two POVOs (and the associated rights) come into conflict due to the fact that:

- The father has the right to hide his health information from whom he wishes, including his child.
- The child has legal rights to know and manage all the information about his health (always within a legal age scenario), including those of hereditary nature belonging to his father.

Any solution invades the rights of one of the parts. In our approach we have resolved that the right of anyone to know all the information related to his/her health has higher priority than the right to show/hide that information to/from others. The implementation of this restriction is shown in the following legal policy:

who:Person(?per) ^ what:Clinical_Information(?inf) ^ attr: Identifiable_Subject(?id) ^ isRelatedTo(?inf,?id) ^ isSubject (?per,?id) → **actionPermitted**(?per,?inf)

The third scenario focuses on the authorship of information about the SoC. Due to the characteristics of the POVO concept, information is obtained from different sources such as monitoring devices, test results from healthcare organizations, genomic information from laboratories, diagnosis and treatment by healthcare professionals, and demographic data, food habits or exercise routines introduced by the SoC. All that information is about the SoC, and he/she has authority to restrict the access to it. The question is whether the author of a piece of information (e.g., a physician who has introduced a diagnosis and personal observations about an SoC) must be able to access that information in the future or, on the contrary, if the SoC can overturn the authorship of the information and deny the access to its authors. We have resolved to always permit an individual to access the information, which he/she has created although the SoC decides to restrict it. We consider that a healthcare professional should be able to revise his/her diagnoses, observations, prescriptions, etc., as a key to the continuity of the assistance and follow-up of SoCs. This rule is applied to all the available health information and not to any information removed by the SoC from his/her POVO. In this case, the information is deleted and nobody can access it, not even its author. The rule specifying this policy is:

who:Person(?per) ^ what:Clinical_Information(?inf) ^ has Author(?inf,?per)
→ **actionPermitted**(?per,?inf)

The technological solution approached in this paper is independent of these decisions and could support other policies. Some exceptional cases have been considered and resolved for our proof of concept, but any case (discussed here or not) must obey current legislation in the moment of use.

4.2. *Future work*

This paper presents a healthcare service oriented architecture supporting SoC-centric assistance and empowering citizens with administration responsibilities. As stated, it is a complex scenario with a lot of issues to address and requirements to satisfy. In this paper, we only introduce design keys and guidelines based on SDOs' efforts to achieve such a scenario, and a great deal obviously remains to be done. Some requirements of POVO scenario will be addressed by adopting future results from SDO such as in the formalization of health information exchange or the conformance with security directives.

We have focused on access control mechanisms trying to show the potential of semantic technologies for easing those complex tasks to SoC without technological skills. A lightweight version of the M3A editor has been presented where the ontology for resource descriptors has not been included in the metamodel for simplicity. Thus, attributes for users and resources must be manually introduced, but in a more evolved version, these shall be eligible for the SoC as another element of the editor. Another future effort will be the development of the M3A editor as a web service allowing ubiquitous policy edition through a web interface.

Furthermore, the POVO paradigm inherits some features of PHR or PCHR approaches but evolves toward a more personalized assistance and actual administration by the SoC. Its key points are the enhancement of interoperability, openness and distribution. Therefore, we consider the use of standardized architectures aligned with standardization efforts and semantic technologies to be a cornerstone for improving interoperability. In this paper we give a technological solution to current (and future) access control issues. Thanks to the application of the RM-ODP principles, the POVO concept is not anchored to the applied technology but it will be able to accommodate future solutions and technologies.

Finally, the approach presented in this paper must face several challenges. Firstly, the collaboration among resource owners, healthcare organizations and third parties should be established through formal security and sharing policies. The definition of administrative boundaries and responsibilities in distributed and collaborative scenarios is a major issue requiring the active participation of all the involved stakeholders. Secondly, a shift of healthcare delivery such as presented here should encourage citizens to be proactive in their health and healthcare professionals to take a secondary role. But both groups can be reluctant to assume these different roles. Moreover, an actual shift of healthcare delivery can lead to technologic ghettos of less technology inclined people. Thus, technology must be at the service of people and not vice versa. Thus, usability and accessibility are two essential features in design and development of end-user systems. Lastly, having a POVO for each citizen requires high processing capabilities, great protection measures, and long-term systems.

As has been approached in this paper, technology could address these challenges in theory but reality is far more complex. A current hurdle is the opposition of systems and processes to a shift in healthcare delivery. A proactive SoC implies, among other things, the restructuration of health processes and the adaptation of current systems to a new scenario; and this change requires a great effort from all stakeholders.

5. Conclusions

A more personalized and user-centric healthcare has been a pressing goal of the scientific community for many years. The resulting approaches are many and diverse covering PHR, PCHR, smart-cards, etc. In this paper we have approached the Person-Oriented Virtual Organization paradigm, taking into account well-known practices and emphasizing issues such as the management of distributed resources, the SoC as administrator, the access decision made by an inference engine upon ontologies and rules, and openness and interoperability concerns. A POVO allows joining all the resources and health information related to an SoC in a coherent whole granting his/her absolute privileges of management only repealed in exceptional scenarios specified by law.

Semantic technologies have been used to support a framework where different systems can communicate without misunderstanding. In addition, they ease the automation of administration tasks such as decision making processes by using inference engines, or the specification of access control policies by using rule languages. A key foundation of this approach is the relationship between technology and end-user, i.e., usability. Through metamodeling and model-to-text transformations, a set of tools has been developed to assist SoCs with various skills to manage the access control to their POVO resources.

The essential cornerstone of the POVO paradigm is a Healthcare Services Architecture following SOA principles (HSOA) and international standards for Healthcare Information Services Architectures. Adopting frameworks and standards can reduce interoperability problems within healthcare scenarios.

Finally, although the POVO concept satisfies the specified requirements, it also presents a set of questions (shown in the previous section) which needs further analysis and will be object of future studies on this topic. Facing the exceptional cases discussed, the authors consider that they have no criterion to establish an absolute solution for each one. Future laws must consider and solve these discussions. In spite of this, the presented access control approach can support every potential solution established by legislative organizations.

Authors' contributions

Jorge Calvillo analyzed the current situation, thought about potential solutions, designed the POVO concept and the architecture, developed access control mechanisms, wrote the manuscript, and reviewed the manuscript. Isabel Román and Laura Roa analyzed the current situation, thought about potential solutions, designed the architecture, and reviewed the manuscript.

Conflict of interest statement

No conflicts of interest occurred.

Acknowledgments

This work has been partially supported by the CIBER-BBN (inside project PERSONA), the Biomedical Engineering Group at University of Seville, an Excellence Project of the Andalusian Council (TIC-6214) and a grant from the 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.

Summary table

What was already known on the topic

- Current trends of technologies centered on the patient aim at granting him/her privileges of administration over all the resources related to his/her health, adopting an active role in the maintenance of his/her well-being. There are different technical solutions in this domain but there are still gaps.
- There are an increasing number of resources (sources and sinks) of knowledge involved in the health of one subject of care. Not only information but also devices or software components. Their heterogeneity and variability make the administration of them a difficult task.
- Other causes influencing this problem are the separate geographic locations, distinct underlying technologies, different administrative domains, etc. Interoperability becomes a complex goal.

What this study added to our knowledge

- By establishing the federation of distributed systems as a base, we have presented the paradigm of Person-Oriented Virtual Organization, which allows joining all the resources and health information related to a subject of care in a coherent whole, granting him/her absolute privileges of management only repealed in exceptional scenarios specified by law.
- Semantic technologies allow automating administration tasks such as decision making processes by using inference engines or the specification of access control policies by using rules languages.
- Usability of solutions is a relevant asset to promote the active role of the SoC, allowing a friendly administration of his/her resources. Meanwhile, transformations from user-level model to machine-processable rules hide the technological complexity from end-users.

REFERENCES

[1] A.W. Ekdahl, L. Andersson, M. Friedrichsen, They do what they think is the best for me. Frail elderly patients' preferences for participation in their care during hospitalization, Patient Educ. Couns. 80 (2) (2010) 233–240.

[2] R. Haux, Individualization, globalization and health—about sustainable information technologies and the aim of medical informatics, Int. J. Med. Inform. 75 (12) (2006) 795–808.

[3] U.S. Government, Health Insurance Portability and Accountability Act (HIPAA), 1996.

[4] International Medical Informatics Association, Code of Ethics for Health Information Professionals, 2002.

[5] Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine, Council of Europe, Strasbourg, 1997.

[6] World Health Organization, A Declaration on the Promotion of Patients' Rights in Europe. European Consultation on the Rights of Patients, World Health Organization, Amsterdam, 1994, pp. 9–14.

[7] European and Commission, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995.

[8] F.L. Maloney, A. Wright, USB-based personal health records: an analysis of features and functionality, Int. J. Med. Inform. 79 (2) (2010) 97–111.

[9] S. Reti, H. Feldman, C. Safran, Governance for personal health records, J. Am. Med. Inform. Assoc. 16 (1) (2009) 14–17.

[10] F. Bourgeois, P. Taylor, J. Emans, D. Nigrin, K. Mandl, Whose personal control? Creating private, personally controlled health records for pediatric and adolescent patients, J. Am. Med. Inform. Assoc. 15 (6) (2008) 737–743.

[11] Markle Foundation. Connecting for Health: The Personal Health Working Group Final Report. Technical Report, 2003.

[12] B.A. Aubert, G. Hamel, Adoption of smart cards in the medical sector: the Canadian experience, Soc. Sci. Med. 53 (7) (2001) 879–894.

[13] T. Erl, SOA Principles of Service Design, Prentice Hall, 2008.

[14] I. Foster, C. Kesselman, S. Tuecke, The anatomy of the grid: enabling scalable virtual organizations, Int. J. High Perform. Comput. Appl. 15 (3) (2001) 200–222.

[15] ITU-T Rec. X.1142 | OASIS XACML v2. 0 Core: eXtensible Access Control Markup Language Version 2.0, 2005. Available from: http://www.oasis-open.org/committees/xacml.

[16] S. Cantor, J. Kemp, R. Philpott, E. Maler, Assertions and Protocols for the Oasis Security Assertion Markup Language (SAML) v2.0, 2005, Available from: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[17] ISO/TS 22600-1, 2:2006 Health Informatics—Privilege Management and Access Control, 2006.

[18] OASIS, Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare Version 1.0, 2009, Available from: http://docs.oasis-open.org/security/xspa/v 1.0/saml-xspa-1.0-os.pdf.

[19] OASIS, Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0, 2009, Available from: http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-os.pdf.

[20] IHE, IHE IT-Infrastructure White Paper—Access Control, 2009.

[21] HITSP. HITSP/SC108—Access Control Service Collaboration, Version 1.1, 2010.

[22] ITU-T. Rec. X.901 Information technology—Open Distributed Processing—Reference Model: Overview, 1997.

[23] ISO12967-1, 2, 3: Health Informatics—Service Architecture, 2008.

[24] ITU-T Rec. X.906 | ISO 19793: Information Technology—Open Distributed Processing—Use of UML for ODP System Specifications, 2008.

[25] R.O. Sinnott, D.W. Chadwick, T. Doherty, D. Martin, A. Stell, G. Stewart, et al., Advanced security for virtual organizations: the pros and cons of centralized vs decentralized security models, in: Proceedings of the 8th IEEE International Symposium on Cluster Computing and the Grid, 2008, pp. 106–113.

[26] F. Kerschbaum, P. Robinson, Security architecture for virtual organizations of business web services, J. Syst. Arch. 55 (4) (2009) 224–232.

[27] A.H. Karp, H. Haury, H.M. Davis, From ABAC to ZBAC: The Evolution of Access Control Models. HP Labs Technical Report, 2009.

[28] J. Calvillo, I. Roman, S. Rivas, L. Roa, Privilege management infrastructure for virtual organizations in healthcare grids, IEEE Trans. Inform. Technol. Biomed. 15 (2) (2011) 316–323.
[29] OMG. Model-Driven Architecture. Available from: http://www.omg.org/mda/.
[30] D. Ferraiolo, D. Kuhn, Role-based access control, in: Proceedings of the NIST-NSA National (USA) Computer Security Conference, 1992, pp. 554–563.
[31] P. Patel-Schneider, P. Hayes, I. Horrocks, OWL Web Ontology Language Semantics and Abstract Syntax, 2004, Available from: http://www.w3.org/TR/owl-semantics/.
[32] I. Horrocks, P. Patel-Schneider, H. Boley, S. Tabet, B. Grosof, M. Dean, SWRL: A Semantic Web Rule Language Combining OWL and RuleML, 2004, Available from: http://www.w3.org/Submission/SWRL/.
[33] T. Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, W. Winsborough, et al., ROWLBAC: representing role based access control in OWL, in: Proceedings of the 13th Symposium on Access Control Models and Technologies, 2008, pp. 73–82.
[34] M. Knechtel, J. Hladik, F. Dau, Using OWL DL reasoning to decide about authorization in RBAC, in: Proceedings of the OWLED 2008 Workshop on OWL: Experiences and Directions, 2008.
[35] D. Trivellato, F. Spiessens, N. Zannone, S. Etalle, POLIPO: Policies & OntoLogies for Interoperability, Portability, and autonomy, in: Proceedings of POLICY'09, IEEE Computer Society, 2009.
[36] N. Elahi, M. Chowdhury, J. Noll, Semantic access control in web based communities, in: Proceedings of the 3rd International Multi-conference on Computing in the Global Information Technology, 2008, pp. 131–136.
[37] H. Shen, A semantic-aware attribute-based access control model for web services, Lect. Notes Comput. Sci. 5574 (2009) 693–703.
[38] T. Priebe, W. Dobmeier, N. Kamprath, Supporting attribute-based access control with ontologies, in: Proceedings of the First International Conference on Availability, Reliability and Security (ARES), 2006, pp. 465–472.
[39] V. Muppavarapu, S.M. Chung, Semantic-based access control for grid data resources in Open Grid Services Architecture-Data Access and Integration (OGSA-DAI), in: Proceedings of the International Conference on Tools with Artificial Intelligence (ICTAI), 2008, pp. 315–322.
[40] M. Amini, R. Jalili, Multi-level authorisation model and framework for distributed semantic-aware environments, IET Inform. Secur. 4 (4) (2010) 301–321.
[41] B. Blobel, Ontology driven health information systems architectures enable pHealth for empowered patients, Int. J. Med. Inform. 80 (2) (2011) e17–e25.
[42] Eclipse: Eclipse Modeling Framework (EMF). Available from: http://www.eclipse.org/emf/.
[43] D. Amyot, H. Farah, J.F. Roy, Evaluation of development tools for domain-specific modeling languages, Lect. Notes Comput. Sci. 4320 LNCS (2006) 183–197.
[44] Eclipse: Graphical Modeling Framework (GMF). Available from: http://www.eclipse.org/gmf/.
[45] D.S. Kolovos, L.M. Rose, R.F. Paige, F.A.C. Polack, Raising the level of abstraction in the development of GMF-based graphical model editors, in: Proceedings of the International Conference on Software Engineering, 2009, pp. 13–19.
[46] MOFScript. Available from: http://www.eclipse.org/gmt/mofscript/.
[47] Model-to-Text (M2T) project. Available from: http://www.eclipse.org/modeling/m2t/.
[48] S. Kou, M.A. Babar, A. Sangroya, Modeling security for service oriented applications, in: ACM International Conference Proceeding Series, 2010, pp. 294–301.
[49] T. Mouelhi, F. Fleurey, B. Baudry, A generic metamodel for security policies mutation, in: Proceedings of the IEEE International Conference on Software Testing Verification and Validation Workshop (ICSTW'08), 2008, pp. 278–286.
[50] J. Karat, C.M. Karat, C. Brodie, J. Feng, Privacy in information technology: designing to enable privacy policy management in organizations, Int. J. Hum. Comput. Stud. 63 (1–2) (2005) 153–174.
[51] Jess rule engine. Available from: http://www.jessrules.com/jess/index.shtml.
[52] H. Knublauch, R. Fergerson, N. Noy, M. Musen, The Protégé OWL Plugin: an open development environment for semantic web applications, in: Proceedings of the Third International Semantic Web Conference, 2004.
[53] CEN/TC 251, EN 13940-1: Health Informatics—System of Concepts to Support Continuity of Care. Part 1. Basic Concepts, European Committee for Standardization, 2006.
[54] The Systematized Nomenclature of Medicine (SNOMED). Available from: http://www.ihtsdo.org/snomed-ct/.
[55] OBO Foundry. The Open Biological and Biomedical Ontologies. Available from: http://www.obofoundry.org/.
[56] Emfatic Language Reference. Available from: http://www.eclipse.org/gmt/epsilon/doc/articles/emfatic/.
[57] Epsilon Validation Language (EVL). Available from: http://www.eclipse.org/gmt/epsilon/doc/evl/.