Privilege Management Infrastructure for Virtual Organizations in Healthcare Grids

Jorge Calvillo, *Student Member, IEEE*, Isabel Román, Sergio Rivas, and Laura M. Roa, *Fellow, IEEE*

***Abstract*—This paper is focused on the management of virtual organizations (VO) inside healthcare environments where grid technology is used as middleware for a healthcare services-oriented architecture (HSOA). Some of the main tasks considered for the provision of an efficient VO management are management of users, assignation of roles to users, assignation of privileges to roles, and definition of resources access policies. These tasks are extremely close to privilege management infrastructures (PMI), so we face VO management services as part of the PMI supporting access control to healthcare resources inside the HSOA. In order to achieve a completely open and interoperable PMI, we review and apply standards of security and architectural design. Moreover, semantic technologies are introduced in decision points for access control allowing the management of a high degree of descriptors by means of ontologies and infer the decision making through rules and reasoners.**

***Index Terms*—Access control, directory services, privilege management infrastructures (PMI), semantic technologies, service-oriented architecture (SOA), virtual organization (VO).**

I. Introduction

COMPUTING when devices and applications in a healthcare organization make their facilities accessible through services, available via public and stable interfaces, integration, and interoperability can be achieved more easily. Furthermore, the development of new and more complex services, which may be composed from elementary ones, offering advanced capabilities to users, should be more effective.

The approach for designing a system providing services to both end-user applications and other services distributed in a network is often called service-oriented architecture (SOA) [1]. A widely accepted definition of architecture is "a formal description of a system, or a detailed plan of the system at component level (including their inter-relationships) to guide its implementation, as well as the principles and guidelines governing its design and evolution over time" [2]. By applying all these ideas to healthcare environments we could refer to healthcare services-oriented architecture (HSOA).

The collaboration between entities in an SOA could be based on the concept of virtual organization (VO) [3], which refers to a dynamic set of entities (individuals, systems, or institutions) distributed across different administrative domains and separated geographically, usually working toward a common goal, defined around a set of resource-sharing rules and conditions. No matter the nature of resources, they all offer their capabilities through service interfaces, and the principle of distribution allows connecting them and composing complex services making separation (administrative, technical, and geographic) transparent to the end user.

Security is a major concern and we could determine who can access to a resource and under which conditions, establishing the rules of resource sharing needed to set a VO. Each resource owner must be able to determine the policies for controlling access and must trust that the enforcement of these rules is guaranteed.

Nowadays, a model focused on the subject of care (SoC) as administrator of his/her information is more and more desirable, in which each individual can decide about the access to information and resources related to him/her. In parallel, legislation establishes scenarios in which the authority of the SoC can be temporally invalidated such as when a risk of public health exists or an emergency that can result in irreversible injuries or death risk.

The current situation, along the progressive distribution of resources across technological, geography and administrative domains, complicates the complete management by the SoC, requiring simpler administration procedures. The use of normalized privilege management infrastructures (PMI) [4] for VO management could provide a foundation upon which mechanisms for services access control within an SOA can be built.

To sum up, in order to achieve the complete interoperability of resources and applications, two issues must be considered.

First, the establishment of a standardized framework and guidelines for the specification and development of systems can encourage the deployment of complex SOA and focus the different worldwide efforts in order to take a step forward in healthcare domain. Second, mechanisms for security and access control are keys to achieve reliable distributed environments. One valuable tool to define a common language easing the automation of administration and decision-making tasks could be semantic technologies, which would allow an SoC to manage his/her own health information and resources.

In the field of PMI supported by VOs, several efforts have been developed. Concretely, numerous initiatives aim to enhance access control in such heterogeneous and complex environments

Manuscript received April 20, 2010; revised July 29, 2010 and October 4, 2010; accepted December 23, 2010. Date of publication; date of current version. This work was supported in part by the CIBER-BBN, the Biomedical Engineering Group in University of Seville and in part by the Fondo de Investigación Sanitaria under Project PI082023.

J. Calvillo and L. M. Roa are with ISCIII Initiative CIBER-BBN and the Biomedical Engineering Group, University of Seville, Seville 41092, Spain (e-mail: laura@esi.us.es; jorgecalvilloarbizu@gmail.com).

I. Román is with ISCIII Initiative CIBER-BBN and the Área de Ingeniería Telemática, Universidad de Sevilla Seville 41092, Spain (e-mail: isabel@trajano.us.es).

S. Rivas is with the Biomedical Engineering Group, University of Seville, Seville 41092, Spain (e-mail: srivasrivas@gmail.com).

Digital Object Identifier 10.1109/TITB.2010.2104160

TABLE I
RELEVANT STANDARDS AND THEIR CONTRIBUTIONS IN THE APPROACHED PMI

Standard	Description	Adoption in the scope of this work
ISO 10181 [14]	Organization of security frameworks and concepts	Source of common security framework
ITU-T X.509 [15]	Public-key and attribute certificate framework	Certificates for privilege management
IETF 4949 [16] IETF 3198 [17]	Internet security glossaries and the security framework in internet community	Source of common security concepts
OASIS XACML [18]	eXtensible Access Control Markup Lang. (XACML)	Source of ABAC schema
OASIS SAML [19]	Security Assertion Markup Language (SAML)	Communication between ABAC schema elements
IETF 3494 [20]	Lightweight Directory Access Protocol (LDAP)	Protocol for certificate directory services
ITU-T X.500 [21]	Concepts of the Directory services	Directory services for certificates
ISO 22600 [4]	Collaboration among several authorization managers	Normalization of the privilege management infrastructure
CEN 13940 [22]	System of concepts to support continuity of care	Basis for the concept ontology
ISO 13606-4 [23]	Security features within electronic health record	Confidentiality levels of ontology
ISO 21091 [24]	Health directory services for security	Healthcare directory services for certificates

either by applying semantic technologies [5], [6] or by means of new security models [7], [8]. Within the healthcare domain, there are some approaches and healthgrid platforms [9]–[13], but the privilege management is mainly delegated to general-purpose middlewares, and efforts are more focused on application of grid technologies in health rather than on the addressing security requirements.

In this paper, we combine and improve past and current efforts in order to specify a PMI supporting healthgrids. To do this, relevant standards for PMI, as well as methodologies for specification of those infrastructures, are analyzed from those of general purpose to those that are focused on healthcare environments. Requirements and approaches are combined with the VO concept and grid technologies, and we propose an access control management infrastructure for healthcare environments based on semantics and standards compliant. Finally, we introduce a scenario from a real project where a legacy system must be included in the proposed privilege management infrastructure.

II. MATERIAL AND METHOD

A. PMI Foundations and Related Standards

As it has been introduced earlier, one of the keys for success of open and interoperable solutions is the adoption of standards in both general and healthcare domains in order to address issues as security and distribution. In Table I, a set of relevant standards from international standardization organizations is shown, explicitly indicating how they have been adopted in the current study. The standardization organizations are: the International Organization for Standardization (ISO), the International Telecommunication Union, the Internet Engineering Task Force, the Organization for the Advancement of Structured Information Standards, and the European Committee for Standardization (CEN).

According to security initiatives, all of them contribute to the common PMI providing concepts or features that have been considered relevant. Each standard included in Table I provides specific security issues not covered (or not so completely) by the others.

In order to ease interoperability and exchange of information, common terminologies have to be considered and adopted. In this paper, we have used the concepts of [22] to build our ontology, but it is possible—and recommended—to extend it with other existing terminologies, for example those of clinical purpose [the systematized nomenclature of medicine (SNOMED) [25], Galen [26], etc.] or biomedical ontologies [27]. Our resulting ontology is focused on basic semantic features of PMI and eases the integration of other health domain more specialized terminologies.

B. HSOA and Standardization

Several paradigms (SOA is one of the most promising among them) have been approached to address the inherent complexity in the distributed computing systems, but the design, development, deployment, maintenance, and evolution of a distributed system are highly complex tasks. Consequently, it is essential that the architecture (and any function necessary to support it) be defined in a set of standards, so that multiple vendors can collaborate in the provision of distributed systems.

Some healthcare architectures' approaches are developed by standardization organizations, like CEN [28] or the Object Management Group [29]. In the healthcare context, the ISO 12967 Health Information Service Architecture (HISA) standard describes an architecture for the integration of healthcare information services. An important basis for the production of this service architecture standard is the reference model-open distributed processing (RM-ODP) methodology [30]. The specifications are formalized avoiding any dependence on specific technological products and/or solutions.

One of the requirements in our research has been that our results were easily incorporated, and interoperable, in the set of information systems of a healthcare organization using standards. The actual implementation of an SOA requires a middleware layer lying between the computing and networking infrastructure and the services in a distributed computing system. This middleware is intended to offer a higher level of abstraction for the underlying computing and networking resources by hiding the distribution and heterogeneity of implementation

technologies. Our research is focused on the use of grid as middleware for the HSOA.

C. Privilege Management in Grid

Globus toolkit is a grid middleware implementation including a security framework (the Globus Security Infrastructure—GSI) [31] that provides common authentication and authorization mechanisms as well as connections to external infrastructures.

The dynamic nature of VO necessitates first automating the discovery of potential providers, then acquiring access rights to certain services, and finally enforcing the access control policy on runtime upon resources allocation. Several initiatives have appeared, such as the community authorization service [32] or the virtual organization membership service (VOMS) [33], which aim to establish control mechanisms by defining groups of users or attributes to reduce the management tasks.

Another emerging approach is to delegate external infrastructures to make access control decision for grid services. The privilege and role management infrastructure standards validation (PERMIS) [34] is an example of a policy based authorization infrastructure.

D. Semantic Technologies

Another crucial cornerstone of completely interoperable and open HSOA is the use of semantic technologies. Following the SOA paradigm, we are considering highly heterogeneous scenarios where the schemas of attributes are complex too. It is unfeasible to come to an agreement with all the resource providers currently (or in the future) involved. By using ontologies describing concepts for resources together with inference engines, we can obtain mainly three advantages. First, SOA characteristics as openness and interoperability are enhanced because of the understanding between different parties is eased. It is achieved by sharing the formal definitions of resources descriptors as ontologies. The administrator will use these descriptors to label the resources of the different VO. Second, by passing an ontology of concepts through a reasoner we can infer new knowledge and add it as explicit relations and elements. Last, by introducing semantic inference in the mechanisms of access control, the development of elements making decisions can be eased. The access control policies would be expressed according to ontologies (resources, user attributes, environment, etc.) and rule languages. So the logic of decision points could be reduced to an inference engine the results of which would be the permission or prohibition of access.

One of the most popular semantic tools is the Web Ontology Language (OWL) [35], a knowledge representation language based on description logic and Resource Description Framework (RDF) representation. OWL covers the specification of ontologies and it has previously been used for the formalization of policies of access control [5], [36], [37]. In order to write rules composed of OWL concepts a special rule language is required and a promising approach is the Semantic Web Rule Language (SWRL) [38] that allows establishing complex relations among properties extending the OWL expressivity. There are current efforts using SWRL in conjunction with OWL to describe access control policies [6], [39].

All the previous works in this field (i.e., use of OWL and SWRL to define policies and decision making) have general purpose and they do not address the specific requirements of access control in such a complex domain as health. In our approach, we use the OWL language to develop an ontology of resource descriptors, involved actors, and context characteristics that can be implicated in the decision of access (as physical location where the access is performed, date and time, purpose of use, etc.). The access control policies have been expressed by means of SWRL rules and tested and executed by using the Jess engine [40] due to its compatibility with Protégé-OWL platform [41] that allowed developing the knowledge base, i.e., OWL ontology and SWRL rules.

SWRL rules for defining policies and reasoning with Jess in a healthcare setting have been also applied in [9]. The main difference with the current study is that they use these tools to harmonize data protection legislation in Europe, and in this paper, an ontology and rules are proposed to ease the management of health information and resources by an administrator who can be the own SoC. Due to the differences on approaches, in this study neither ontology nor rules could be reused from previous efforts and they have been completely built from the perspective of this paper.

III. Results

A. Security Infrastructure and Use Cases

The approached security infrastructure is based on the standards, methodologies, and technologies revised earlier. We have combined and improved them in order to build an open and complete solution. On one hand, it uses the eXtensible Access Control Markup Language (XACML) specification [18] adding crucial elements centered on semantic management. The result is the services decomposition in Fig. 1, an improved revision of the XACML standard. On the other hand, the authorization schema follows the guidelines of the attribute-based access control (ABAC) access control schema, in which privileges are grouped in attributes, and each individual is assigned a set of those. In our approach, those attributes are specified in a concept ontology described in the next section.

Another important point we include in this revision of the XACML standard is the consideration of separate and distributed policy information points (PIP). Each one follows its own functional protocol (centered on a particular kind of attributes, receiving requests, and sending information) and it is connected to the related knowledge base. Following this trend, the proposed infrastructure replaces centralized components of the XACML schema with services that can be distributed and decomposed in other simpler services. From an architectural point of view, Fig. 1 shows services from different layers of the HSOA. Thus, policy enforcement point (PEP) services directly related to resources belong to the infrastructure layer; services as context handler easing distribution and location are part of middleware layer; resource and environment knowledge bases, PIP services, and policy decision point (PDP) services, all belong to

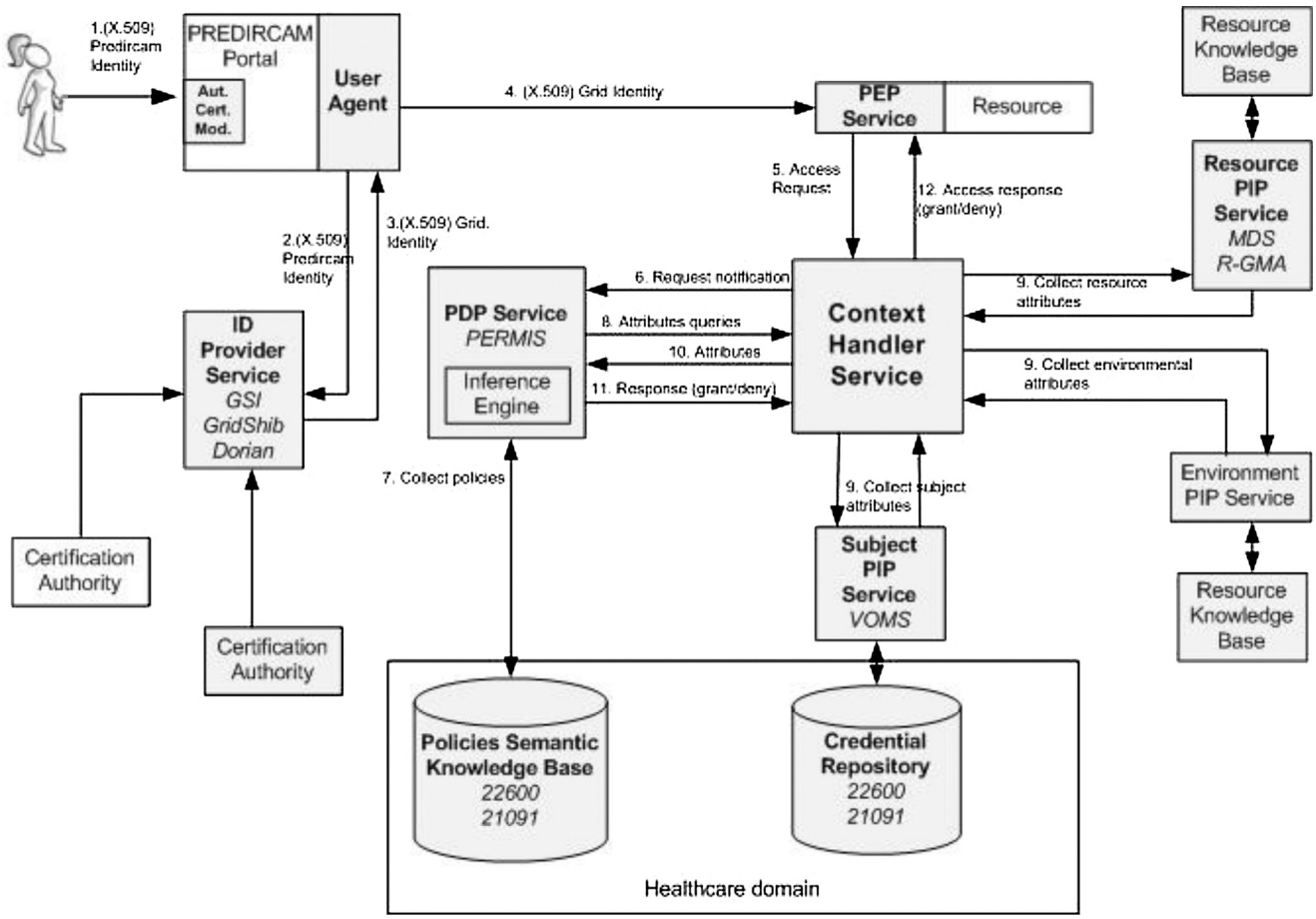

Fig. 1. Use case 1: using a grid service through the PREDIRCAM portal.

the generic service layer; finally, the credential repository and the policies semantic knowledge base are part of the healthcare domain services layer because of their functionality and content are specifically defined to this domain.

According to implementation and technology, although there exist several approaches to address privilege management in grid, in many cases these only present partial solutions of the whole concern. In general, efforts are driven to provide PMI common to all grid services. In actual healthcare systems, even with grid infrastructures deployed, there are several heterogeneous systems whose adaptability to grid is not feasible. Generally, each system has its local privilege management or access control and it does not want delegate access decision to third parties.

We have met this issue in the PREDIRCAM project [42], which is developing and validating an intelligent platform of biomedical technologies for monitoring, prevention, and personalized treatment of mellitus diabetes, the cardiac and metabolic risk, and the renal insufficiency. One of the main components of the platform for PREvention DIabetes and CArdioMetabolic Risk (PREDIRCAM) project is the platform for following up of exercise routines and food habits of patients. This platform has been developed using the Content Manager System (CMS) Drupal [43] version 6. Drupal follows a scheme completely centralized with a local database storing contents of CMS.

Incompatibilities appear when we try to introduce Drupal in the grid infrastructure because the former provides its own user management with local permission through login and password, and the latter uses a public key infrastructure with X.509 certificates to authentication and attribute certificates to authorization.

To integrate autonomous systems with their own local privilege management in the grid we have reviewed three use cases: the system acting as client of a grid service, the system being a service with local privilege management that is accessed by a grid client, and finally, the system as a service accessed by a grid client, but the access control is managed by the global grid infrastructure. Fig. 1 shows the first use case where the system (in our particular case, the PREDIRCAM platform) acts as a client of a grid service, thanks to grid user capabilities delegation. We show the main components in the designed authentication and authorization infrastructure. This approach is flexible and scalable and it facilitates the management of different identities for the same user and the single sign on. Moreover, PIP services for resource, environment, and subject, and PDP services are all independent elements, adding flexibility to the management of VO. In the actual implementation of this architecture every functional element can be distributed in the grid, in order to prevent the dependence in centralized elements.

We have selected and adapted technical solutions for each functional element. For example, identity provider and

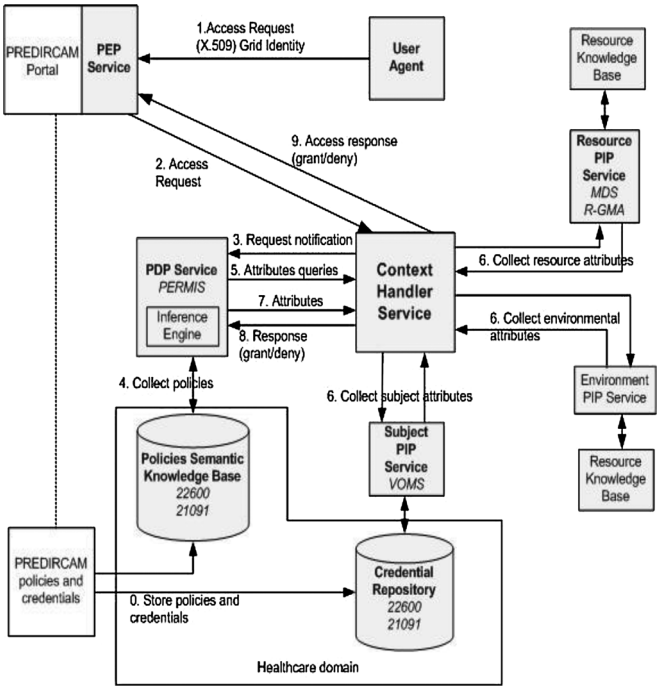

Fig. 2. Use case 2: using PREDIRCAM portal facilities using local security.

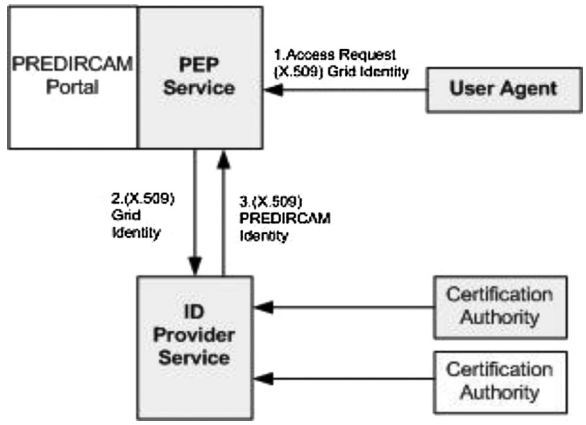

Fig. 3. Use case 3: using PREDIRCAM portal facilities published as grid service using grid privilege management infrastructure.

delegation elements are provided by the Globus Security Infrastructure. An efficient PDP service is implemented in PERMIS and the subject PIP service is based on VOMS. Resource PIP service is based in the Globus Monitoring & Discovery System (MDS) [44]. The context handler service belongs to middleware and it deals with the distribution and location of the different services; thus, it can be implemented in several ways and even it could be integrated in PDP and PIP services. For the sake of simplicity, in the proposed infrastructure Globus MDS performs tasks for discovering and communicating between the different PIP, PEP, and PDP services.

In our approach, the federation and autonomy of systems is facilitated because legacy services could be integrated and they can choose between adopting grid security infrastructure or maintaining their own, as depicted in Figs. 2 and 3. The first one shows the use case in which the legacy system exports some interfaces to grid infrastructure but holding its local privilege management. In Fig. 3, we achieve the integration by modifying the legacy system in order to use the privilege management infrastructure of grid.

Finally, in PREDIRCAM project we have adopted the solution of Fig. 3, and the first step to achieve the integration between the platform and the grid infrastructure is to make the authentication in Drupal accepts X.509 certificates. To provide Drupal with certificate capabilities, we have added the "login certificate" module [45]. Now our legacy system (i.e., Drupal) allows the registration of new users or the access of registered users to the resources protected by the PMI using X.509 certificates, and all this without making any change to the database of the CMS.

B. Ontology and Policies for Controlling Access

To achieve the variability degree required by access control policies, we have modeled an ontology of healthcare domain fulfilling all the potential features of categorization of resources. By using this ontology, the administrator (potentially the SoC) can have a versatile control over the access to resources through the potential actors who can access, the nature of the information, creation dates, authors, physical location of access, purpose of use, etc.

An overview of the developed ontology is shown in Fig. 4. It is composed of: an ontology of healthcare actors, another focused on resource descriptors, and a third one about security used to create the access control policies. Fig. 4 includes the potential actors who can try to access to protected objects (people, organizations, or devices), the two categories of objects to which the access must be controlled (information and resources), and a spectrum of descriptors to characterize these objects (pointing its nature, anonymization level, related disease, availability for different purposes, etc.).

As it has been exposed earlier, policies ruling the access to resources are defined by means of SWRL language and based on the concept ontologies. 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 if the requested action is permitted or prohibited. An example of policy is "allow my partner to see all my information related to sexually transmitted diseases since year 2000 and in which third persons are not involved," that is expressed in SWRL as follows:

$$\begin{aligned} &\textit{who:Person(?per)} \wedge \textit{who:hasRelation(?per, who:SPOUSE)} \wedge \\ &\textit{what:Clinical\_Information(?inf)} \wedge \textit{attr:Sexual\_Organs(?dis)} \\ &\wedge \textit{isRelatedTo(?inf, ?dis)} \wedge \textit{attr:Subject\_Of\_Care(?soc)} \wedge \\ &\textit{isRelatedTo(?inf, ?soc)} \wedge \textit{what:creationTime(?inf, ?time)} \wedge \\ &\textit{temporal:notBefore(?time, "2000-1-1")} \\ &\rightarrow \textit{actionPermitted(?per, ?inf)} \end{aligned}$$

The interpretation of a rule as previous one is: if conditions specified in antecedent are true (i.e., there are OWL individuals satisfying all clauses), then the property "actionPermitted"

Fig. 4. Overview of ontology of healthcare domain concepts.

(or "actionProhibited") must be created among actor/s and resource/s. This process of checking rules and creating properties is realized by the inference engine Jess as it is explained later.

The process of decision making performed by PDP service is: when it receives all the information from PIP services through context handler service, it combines the ontology with SWRL rules, and the Jess engine executes the inference. The inferred axioms are incorporated to the ontology, and the Semantic Query-Enhanced Web Rule Language (SQWRL) is used to verify the existence of the properties "actionPermitted" and "actionProhibited" between the access requester and the requested resource (e.g., actionPermitted(SPOUSE,?p) → sqwrl:select(?p)). After obtaining the results from SQWRL queries, the possible scenarios are as follows.

1) There is a property of permission (or prohibition); then the decision of acceptance (denegation) of access is made.
2) Two or more policies defined by the SoC are incoherent, and there exist the two properties (permission and prohibition) at the same time; the more conservative decision is made (i.e., denying the access).
3) There is no policy ruling the requested access, and any decision cannot be made; we solve this scenario by making the PDP to deny the request and communicating to the SoC to specify (if he/she will) the rule controlling this kind of access.

C. Normalization and Architectural Design

We have considered in all scenarios what health informatics standards are established. For example, in our infrastructure it is essential that lightweight directory access protocol (LDAP) repositories conform to [4] and [24]. Moreover, the results described earlier (i.e., security infrastructure, specification of policies, and access decision making) have been developed within a normalized architecture following principles of interoperability and openness. As was presented in the section of methodology, RM-ODP and HISA have been chosen for the normalization of the healthcare services architecture supporting our approach. This standard formalizes only fundamental aspects, which are common and currently essential in any advanced healthcare system, so it has been extended in different features.

Fig. 5 shows the fulfillment between actors and roles within the Security Infrastructure Community, the scope of which is to establish a controlled access to protected resources by means of policies. Among the relevant actors there are some systems (ID provider, context handler, policy enforcement, information, and decision) and entities related to people or organizations (resource owner, user, and user agent). The enterprise viewpoint abstracts from real implementations or use cases and it presents entities involved in the security infrastructure community covering all possible scenarios. The functionality of each actor in the community is described by the role/s that the actor fulfills. The available roles are: requester, identity provider, decision agent, resource and policy admin, resource access manager, context manager, etc.

This diagram is part of the normalization of the enterprise viewpoint described by HISA, RM-ODP, and the standard ISO 15414 [46] providing the proper enterprise language. All the components supporting the access control in our approach have been designed as services inside the HSOA, by using the ISO 19793 standard [47] for their inclusion and formalization in the different ODP viewpoints, and improving their reutilization and scalability.

Information and computational viewpoints inherit directly from HISA standards including also the framework of common concepts and systems established by the standards described in

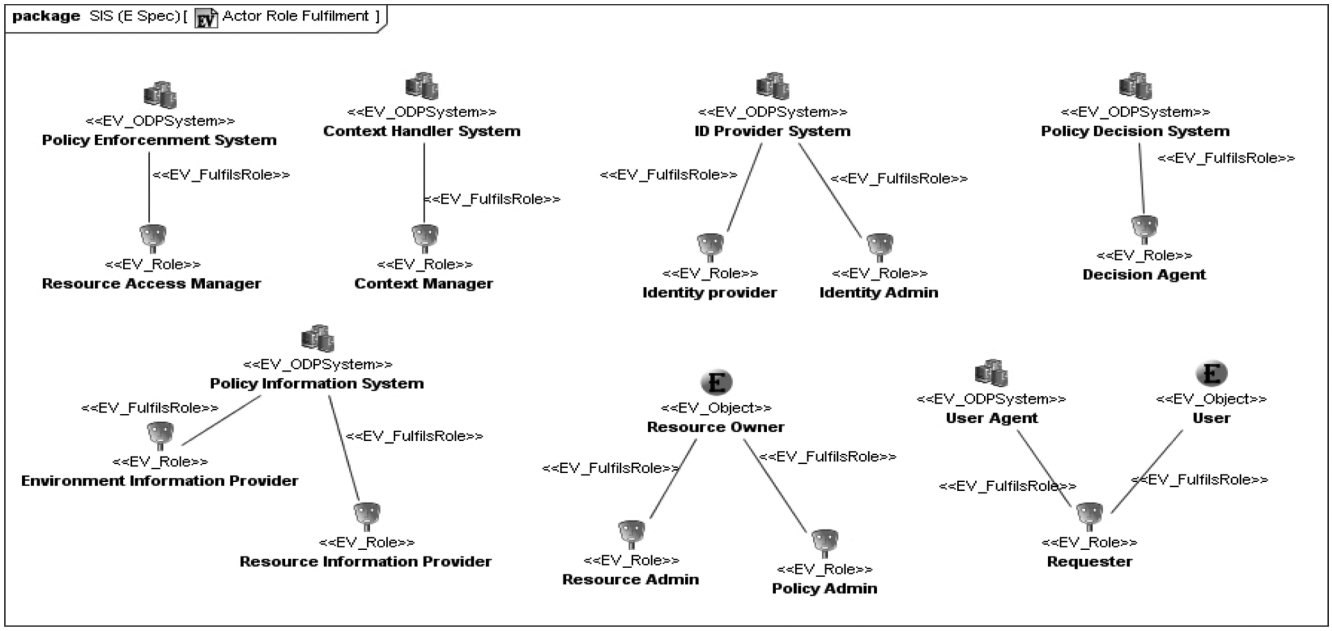

Fig. 5. Actor role fulfillment and assignment rules.

Section II-A. Engineering and technology viewpoints deal with implementation issues and specify how grid technologies (in our case, the Globus middleware) provide the capabilities of our privilege management infrastructure. Although in this study, a real implementation with grid technologies has been described, the formalization of the infrastructure by using ODP allows other middleware technologies to be used. Thus, only engineering and technology viewpoints would have to be provided.

A more detailed specification of the viewpoints of our approach will be the focus of future studies.

IV. Conclusion

Our study has been focused on the development of a healthcare PMI that an SoC could administrate, i.e., he/she could decide about the access to his/her health resources. How this scenario is achieved it is what the authors consider the great contribution of this paper.

Throughout the entire process of development (from design to implementation), several contributions can be remarked. In the first stage and having the openness and interoperability as crucial requirements, numerous standards (of security, architecture formalization, terminologies, etc.) have been analyzed. The most relevant ones have been combined and enhanced in order to build a semantic based PMI. Traditional and centralized approaches as XACML and role-based access control (RBAC) have been improved by considering the distribution and composition of services following the SOA paradigm, and also the semantic management in decision points of access control allowing automating administration tasks. In this phase, the PMI has been formalized according to ODP and HISA standards. Although the latter is healthcare domain specific, it does not consider security issues, and in this study an extension of it has been necessary. Due to this formalization is normalized and technology independent, the resulting PMI can be implemented by means of different platform and technologies, and all the implementations retain the same levels of interoperability, scalability, and openness.

In a second stage, three use cases have been analyzed in order to study the openness of the PMI and the potential integration of legacy systems with it. These use cases allowed extracting functional requirements for both the PMI and the legacy system, stressing the adequacy of considering the problem of legacy system integration in an early stage of the system design.

The next phase has focused on the implementation, and the PMI services have been particularized like concrete technological elements. Grid technologies have been selected as underlying middleware and all the components have been adapted to work together and be conformed to selected standards supporting the designed PMI in the first stage. In parallel, a concept ontology has been developed to support the access control mechanisms of PMI. Moreover, SWRL has been used as policy language and it has been shown how semantic technologies (ontologies, inference engines, and rule languages) could automate administration tasks and facilitate a flexible and scalable management of dynamic VOs.

Finally, our implemented PMI has been proved in a real project (PREDIRCAM). We have faced the integration of a legacy system with the PMI and the solution of the third use case was a success. To achieve this, the legacy system was adapted to manage X.509 certificates and be able to communicate with the whole PMI and protected resources, delegating the access control to the normalized platform.

References

[1] T. Erl, *SOA Principles of Service Design*. Englewood Cliffs, NJ: Prentice-Hall, 2008.

[2] The Open Group. (2009). TOGAF, Enterprise edition, version 9. [Online]. Available: http://www.opengroup.org/architecture/togaf9-doc/arch/index.html.

[3] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the grid: Enabling scalable virtual organizations," *Int. J. Supercomput. Appl.*, vol. 15, no. 3, pp. 200–222, 2001.
[4] *Health Informatics—Privilege Management and Access Control*, ISO 22600-1,2, 2006.
[5] D. Trivellato, F. Spiessens, N. Zannone, and S. Etalle, "POLIPO: Policies & OntoLogies for interoperability, portability, and autonomy," in *Proc. Policy, IEEE Comput. Soc.*, Jul., 2009, pp. 110–113.
[6] N. Elahi, M. Chowdhury, and J. Noll, "Semantic access control in web based communities," in *Proc. 3rd Int. Multi-Conf. Comput. Global Inform. Technol.*, Jul./Aug., 2008, pp. 131–136.
[7] N. Zhang, L. Yao, A. Nenadic, J. Chin, C. Goble, A. Rector, D. Chadwick, S. Otenko, and Q. Shi, "Achieving fine-grained access control in virtual organizations," *Concurrency Comput.: Pract. Exper.*, vol. 19, pp. 1333–1352, 2007.
[8] R. Sinnott, D. Chadwick, T. Doherty, D. Martin, A. Stell, G. Stewart, L. Su, and J. Watt, "Advanced security for virtual organizations: The pros and cons of centralized vs decentralized security models," in *Proc. 8th IEEE Int. Symp. Cluster Comput. Grid*, May, 2008, pp. 106–113.
[9] H. B. Rahmouni, T. Solomonides, M. C. Mont, and S. Shiu, "Ontology-based privacy compliance on European healthgrid domains," *Stud. Health Technol. Informat.*, vol. 147, pp. 183–189, 2009.
[10] I. Román, L. Roa, L. Reina, and G. Madinabeitia, "Demographic management in a federated healthcare environment," *Int. J. Med. Inf.*, vol. 75, no. 9, pp. 671–682, 2006.
[11] D. Krefting, J. Bart, K. Beronov, O. Dzhimova, J. Falkner, M. Hartung, A. Hoheisel, T. Knoch, T. Lingner, Y. Mohammed, K. Peter, E. Rahm, U. Sax, D. Sommerfeld, T. Steinke, T. Tolxdorff, M. Vossberg, F. Viezens, and A. Weisbecker, "MediGRID: Towards a user friendly secured grid infrastructure," *Future Generat. Comput. Syst.*, vol. 25, no. 3, pp. 326–336, 2009.
[12] D. J. Power, E. A. Politou, M. A. Slaymaker, and A. C. Simpson, "Towards secure grid-enabled healthcare," *Softw. – Practice Exp.*, vol. 35, no. 9, pp. 857–871, 2005.
[13] D. Olmedilla, O. Rana, B. Matthews, and W. Nejdl, "Security and trust issues in semantic grids," in *Proc. Dagsthul Semin. Semi. Grid: Convergence Technol.*, 2005, p. 05271.
[14] *Information Technology—Open Systems Interconnection—Security Frameworks for Open Systems,* ISO 10181-1,2, 1996.
[15] *The Directory: Public-Key and Attribute Certificate Frameworks,* ITU-T Rec. X.509, 2008.
[16] *Internet Security Glossary,* RFC 4949, version 2, 2007.
[17] *Terminology for Policy-Based Management,* RFC 3198, 2001.
[18] OASIS. (2005). XACML v2.0 Core, eXtensible Access Control Markup Language Version 2.0, OASIS. [Online]. Available: http://www.oasis-open.org/committees/xacml.
[19] S. Cantor J. Kemp R. Philpott E. Maler. (2005). Assertions and protocols for the oasis security assertion markup language (SAML), v2.0, [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.
[20] *Lightweight Directory Access Protocol,* version 2, RFC 3494, 2003.
[21] The Directory: Overview, ITU-T Rec. X.500, 2008.
[22] *Health Informatics—System of Concepts to Support Continuity of Care—Part 1: Basic Concepts*, European Committee for Standardization, CEN/TC 251, EN 13940-1, 2006.
[23] Health Informatics—Electronic Health Record Communication—Part 4: Security, ISO 13606-4, 2007.
[24] *Health Informatics—Directory Services for Security, Communications and Identification of Professionals and Patients,* ISO 21091, 2005.
[25] *The Systematized Nomenclature of Medicine (SNOMED)* [Online]. Available: http://www.ihtsdo.org/snomed-ct/.
[26] A. Rector and W. Nowlan, "The GALEN project," *Comput. Methods Programs Biomed.*, vol. 45, no. 1–2, pp. 75–78, 1994.
[27] OBO Foundry. (2010, Jul.). "The open biological and biomedical ontologies," [Online]. Available: http://www.obofoundry.org/.
[28] Health Informatics – Service Architecture, ISO 12967-1,2,3, 2008.
[29] CORBAmed OMG. (2010, Jul.). HDTF standards [Online]. Available: http://healthcare.omg.org/Roadmap/corbamed_roadmap.htm.
[30] *Information Technology—Open Distributed Processing—Reference Model,* ISO 10746-1,2,3,4, 1998 (Revised in 2010).
[31] Globus Toolkit Security. (2010, Jul.). [Online]. Available: http://www.globus.org/toolkit/docs/latest-stable/security/.
[32] I. Foster, C. Kesselman, L. Pearlman, S. Tuecke, and V. Welch, "The community authorization service: Status and future," presented at the Proc. of the Comput. in High Energy Physics, La Jolla, CA, Mar. 2003.
[33] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Frohner, K. Lorentey, and F. Spataro, "From gridmap-file to voms: Managing authorization in a grid environment," *Future Generation Comp. Syst.*, vol. 21, no. 4, pp. 549–558, 2005.
[34] Permis (project funded by the ISIS program). (2010, Jul.). [Online]. Available: http://www.permis.org/index.html.
[35] P. Patel-Schneider, P. Hayes, and I. Horrocks. (2004). OWL web ontology language semantics and abstract syntax, [Online]. Available: http://www.w3.org/TR/owl-semantics/.
[36] T. Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, W. Winsborough, and B. Thuraisingham, "ROWLBAC: Representing role based access control in OWL," in *Proc. 13th Symp. Access Control Models. Technol.*, Jun., 2008, pp. 73–82.
[37] M. Knechtel, J. Hladik, and F. Dau, "Using OWL DL reasoning to decide about authorization in RBAC," in *Proc. OWLED Workshop OWL: Experiences and Directions*, 2008.
[38] I. Horrocks, P. Patel-Schneider, H. Boley, S. Tabet, B. Grosof, and M. Dean, 2004. SWRL: A semantic web rule language combining OWL and RuleML, [Online]. Available: http://www.w3.org/Submission/SWRL/
[39] H. Shen, "A semantic-aware attribute-based access control model for web services," *Lect. N. Comput. Sci.*, vol. 5574, pp. 693–703, 2009.
[40] Jess Rule Engine. (2010, Jul.). [Online]. Available: http://www.jessrules.com/jess/index.shtml.
[41] H. Knublauch, R. Fergerson, N. Noy, and M. Musen, "The protégé OWL plugin: An open development environment for semantic web applications," in *Proc. 3rd Int. Semantic Web Conf.*, 2004, pp. 229–243.
[42] P. Herrero, M. E. Hernando, L. Roa, E. Gómez, and A. de Leiva, "PREDIRCAM: Technological platform for the prevention of diabetes mellitus and cardioMetabolic risk," presented at the 2nd Conf. on Advanced Technologies and Treatments for Diabetes, 2009, Athens, Greece.
[43] CMS Drupal. (2010, Jul.). [Online]. Available: http://drupal.org.
[44] MDS. (2010, Jul.). [Online]. Available: http://www.globus.org/toolkit/mds/.
[45] Login Certificate Module. (2010, Jul.). [Online]. Available: http://drupal.org/project/certificatelogin.
[46] *Information Technology—Open Distributed Processing—Reference Model—Enterprise Language,* ISO 15414, 2006.
[47] *Information Technology—Open Distributed Processing—Use of UML for ODP System Specifications,* ISO 19793, 2008.

Author's photographs and biographies not available at the time of publication.