Prosumer's Responsibilities?... On Stage to a Dedicated Framework for Services Sharing and Compliance in the Healthcare Domain.

Khadraoui, Abdelaziz; Nicolas, Damien; Feltus, Christophe

DOI:
10.4018/978-1-4666-4313-0.ch006

Publication date:
2013

Document Version
Early version, also known as pre-print

Prosumer's Responsibilities?... On Stage to a Dedicated Framework for Services Sharing and Compliance in the Healthcare Domain

Abdelaziz Khadraoui*, Damien Nicolas, Christophe Feltus****

(*) (✉) Institute of Services Science, Centre Universitaire d'Informatique, University of Geneva, Switzerland
e-mail: abdelaziz.khadraoui@unige.ch
(**) Public Research Center Henri Tudor, Luxembourg-Kirchberg, Luxembourg
e-mail: damien.nicolas@tudor.lu; christophe.feltus@tudor.lu

ABSTRACT

This chapter addresses issues relating the clarification of responsibilities associated to business services. The definition of the constraints is part of the definition of the services.
Our main objective is to describe the influence of the constraints in the service elaboration mechanisms. We propose an approach for the specification of the constraints associated to services and for the management of access rights needed to use and exploit services. The usage of services is strongly coupled with the stakeholder's responsibilities.
Finally, we discuss a usage scenario implementing this approach, in the context of sensitive data exchange between stakeholders from the healthcare domain. Furthermore, we describe how the constraints are defined.

1 INTRODUCTION

For the last decade, proactive consuming has considerably affected economic models and has positively influenced the development chains of the production of hi-tech material and highly sophisticated products. Although actually roughly considered by the production industry of tangible goods, prosumering has for a long time remained in the shadow of the production of services. On stage to integrate this consuming/producing dimension in the architecture of service science frameworks, our work intends to enrich the forthcoming theory related to the service sharing along two dimensions: the responsibility of the prosumers and the needs for compliance with legal framework and organizational constraints. The services compliance aims to improve the quality of services to be offered to the stakeholders and users concerned by these services.

By definition, a prosumer is made performing a larger set of activities related to the service, whether it is in service definition or in service exploitation. Those activities are defined by a set of obligations assigned to the prosumer, for which a certain commitment is expected, and for which capacity are required. In the field of service, differently as in the field of tangible good, the prosumer is more often hired in an institution or in a company and, thereby is often more solicited to give account to an authority regarding the achievement of its obligations.

For example, in the field of healthcare, service consuming is of flashy color since having access to services is sometimes crucial for the life of the patient. Therefore, healthcare employees are often on a food war to manage their access to the service, to enhance the service performance and to take the service expected output as far as it is needed to the extent of their work.

The management of the access to patient files in the healthcare sector is of huge importance since the manipulated data concern very sensitive and confidential personal information. In Luxembourg, this personal data protection has been legitimated by the national law of August the 2nd, 2002. All actors working in the healthcare field have the legal constraints to conform to this law.

In our previous research we launched works about the analysis of the service compliance and about the definition of integrated IS architectures in order to support the service compliance analysis [1], [2], [3]. In [1], we proposed a novel approach which permits to establish a strong link between the organizational layer and the informational layer of a service, and to clarify the responsibility dimension in order to guarantee the compliance of services.

In this chapter, we consolidate the proposed approach and we address a specific challenges concerning the definition of the constraints and the definition of the responsibility aspects of the stakeholders and users involved in services in the perspective to establish a compliance between services and the domain constraints.

The rest of the chapter is organized as follows: in section 2 we describe how the responsibility is modelled. In section 3 we present the dynamic constraint model and we discuss generic types of constraints as depicted in the literature. In section 4 we illustrate our proposed approach for the specification of the constraints associated to services and for the management of access rights needed to use and exploit services by prosumers. Section 5 describes a simplified usage scenario illustrating the proposed approach. Finally, in section 6 we conclude and present future perspectives of this work.

2 MODELING RESPONSIBILITY

The elaboration of the responsibility meta-model (Figure 1) has been performed based on a literature overview. As explained in previous papers [2], we have, in the first place, analyzed how responsibility is included in information technology professional frameworks, in the field of requirements engineering and role engineering, and in the field of access right with the review of access control models. Afterwards, this literature overview has been completed by a literature review in the field of Human Sciences (psychology, sociology, and management).

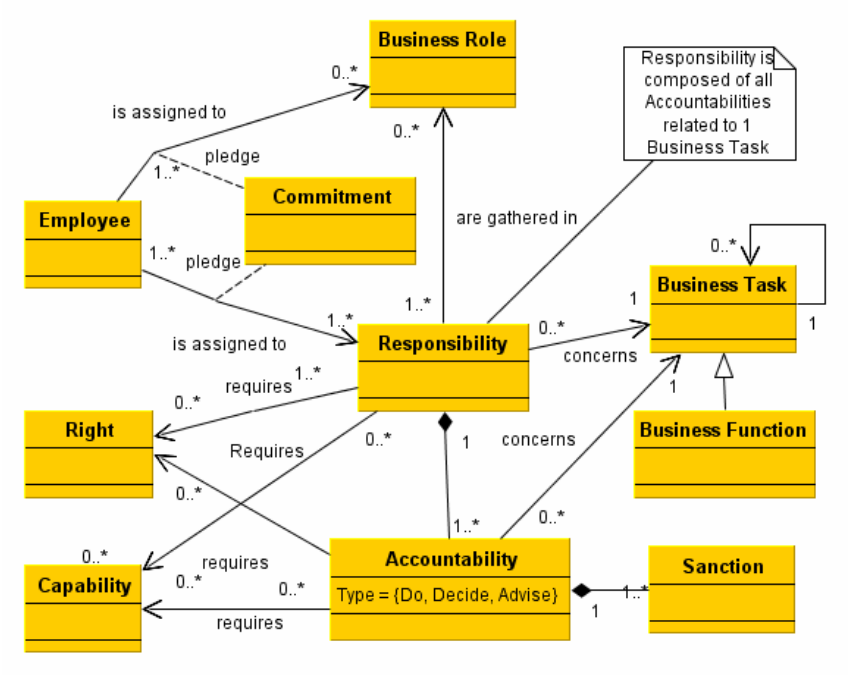

Figure 1. *Responsibility* modelled in UML.

In figure 1, the most meaningful concepts are defined in the following way:

- The **responsibility** is a charge assigned to an employee to signify his accountabilities concerning a business task, and the right and capacity required to perform those accountabilities.
- The **accountability** represents the obligation of what has to be done concerning a business task and the justification that it is done to someone else, under threat of sanction
- The **capability** represents the qualities, the skills or the resources intrinsic to the employee and required to perform accountability.
- The **right** represents the resources provided by the company to the employee and required to perform accountability.
- The **assignment** is the action of linking an agent to a responsibility. Delegation process is the transfer of an agent's responsibility assignment to another agent.

3 CONSTRAINT MODEL

The development of the service model and the responsibility model, as well as the integration of both, has been realized independently of the context in which it is applied. Thereby, both of them do not consider the context specificities. In order to ease the deployment and sharing of services/responsibilities, this section provides an organic picture of those constraints collected in a so called Dynamic Constraint Model (DCM).

Six types of constraints have been identified in the DCM for impacting the service/responsibility sharing. These six constraints are organized in two areas: The Domain Constraints and the Organizational Context (domain). The Domain Constraints gather (1) the Law constraints – eg.: in the finance sector, Sarbanes Oxley Act constraints CEO to access operating results, (2) the Business framework – eg.: non-mandatory business frameworks such as CobiT request to have accountabilities and responsibilities of the employees well defined regarding the management of the IT security. This constraint has a direct impact on the access right to the information accessed in the frame of a service, (3) Domain regulation – eg.: specific domain regulation also brings well precise type of constraints – eg.: the national law of August the 2nd, 2002 have an impact on all healthcare actors in Luxembourg, (4) Legacy role constraints the company to define a role with precise legal duties and constraints – eg. In the pharmaceutical industry, drug production must be under the supervision of a head pharmacist always, and (5) Organizational Domain Constraints that have been identified as constraints imposed at the organizational layer due to the domain of activity – eg.: In public administration, the organizational rules (in terms of hierarchy) and the services sharing are strongly associated to the domain constraints. This is the case when civil aviation authorities that produce airworthiness directives under the cover of a government. The Organizational Context gathers the same constraint (5) as the Domain Constraint and (6) the Organizational Specific Constraint that are imposed following internal company rules such as, eg.: the ordering of material for an amount higher than 20.000 euros requests the signature of at least two employees.

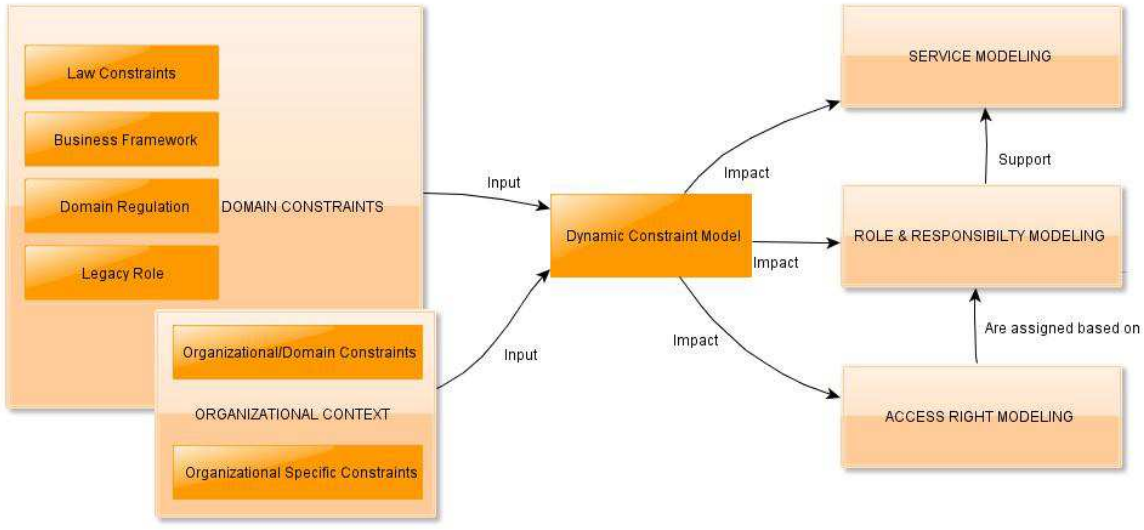

Figure 2. Dynamic Constraint Model.

Towards a generic constraints topology

Generic constraints have been identified from the literature. Those constraints form a portfolio of generic constraint are useable to tailor domain specific ones. Those generic constraints are:

- The cardinality constraint [7] that implies a maximum or a minimum of occurrence of an element of the service/responsibility, this constraint requires for instance having not to many responsibilities assigned to a unique employee, to have at least two of them involved in the critical decision making process, and so forth.

- The separation of duties constraint [6] aims at constraining the realization of an action to be achieved by at least two roles, or two employees. This is classically the case of the material ordering process that asks for having at least two stakeholders involved, one for the ordering, and the other for the invoicing. At the very technical layer (including technical access rights management model), this constraint may be either a statistic or a dynamic separation.

- The delegation constraint [8] [9]. The delegation of responsibilities is also an activity strongly framed with certain delegation rules. These delegation rules aim at structuring the delegation between two stakeholders and clarifying what delegation is allowed, between whom, under what conditions, etc.

- The accountability rules [2] aim at determining who keeps the accountabilities of tasks when operations are performed. For instance, if an employee accepts a new responsibility, to who is he constrained to answer, what are the consequences of this constraint in terms of sanctions, and so forth.

- The commitment constraint [2]. This last type of constraint is linked to the assignment of responsibilities. Indeed, depending on the type of responsibility, a stakeholder may be more or less requested to pledge a hard or soft commitment.

Practically, these 5 generic types of constraints have been depicted in the literature and are existing, instantiated, detailed or expended through legal or organizational frameworks. Official papers and requirements arguing more for constraints such as the separation of duties, accountability rules or cardinality constraints and less official one (such as book of good practices or recommendations) arguing more for delegation constraint, commitment constraint and cardinality constraint as well. In parallel to these 6 generic constraints, additional ones could be recovered in the literature but they are more specific to certain domains. This is for instance the case of the “Chinese wall” “constraint” which is more dedicated to administration area.

The definition of the service/responsibility model in this section lets room for constraint consideration. Therefore, figure 2 has been drawn to give an insight of the influence of theses constraints in the service elaboration mechanisms. This figure highlights that the constraints have an effective impact on the three layers of the mechanisms. At the service modeling layer, the modularity of the service structures are highly depending on the cardinality constraint so that a service as a sufficient granularity level to be exactly assigned to the stakeholders. Without such a granularity, it is impossible to provide precise access to the employees, nor to give them access to a precise set of access rights. At the responsibility layer, the impact of the constraint model is also meaningful. Indeed, in the definition of the responsibility stage, it is

important to keep in mind the requirement not to have too much responsibility in the hand of a unique role (delegation of duty), to precise in the responsibility the expected commitment level of the stakeholder, or the delegation level allowance. Finally, the constraint model as an impact on the access rights models, including the alignment mechanism of these access rights (model) with the responsibilities (and thereby the services). At this level, some constraints are no longer taken into account since there existence is justified only at the organization level. However, others constraints are strengthened like the separation of duty that is operationalized at that level or the cardinality.

4 THE USAGE OF SERVICES BY PROSUMERS

The usage of the specified services is strongly coupled with the stakeholder's responsibilities. The definition of the responsibilities as presented previously is a crucial issue. This task permits to determine the obligations to be assigned to the stakeholders according to the organizational processes. The figure below illustrates our proposed approach for the specification of the constraints associated to services and for the management of access rights needed to use and exploit services.

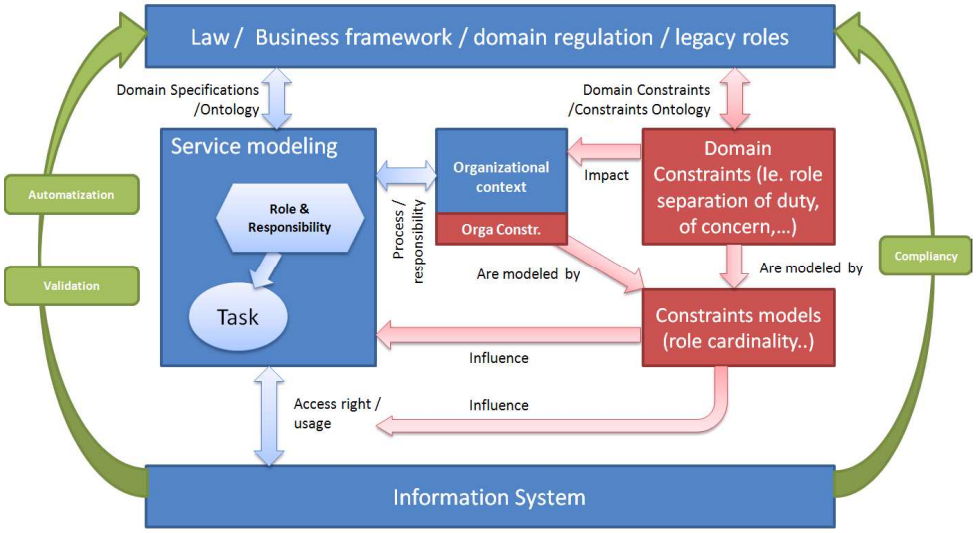

Figure 3. The usage of services

To have a compliance between the business Information System that supports services and the Business layer at the genesis of those services (through business framework, law and domain regulation mainly) must be modeled according to domain specifications and ontology.
As described in figure 4, the modeling of services includes several tasks.

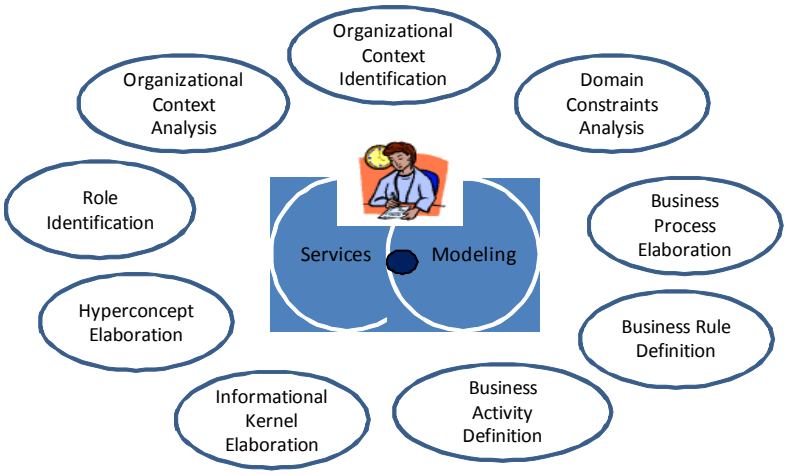

Figure 4. Service modelling

Service architects are involved in the identification organizational context and the analysis of domain constraints , in the definition of business rules and business activities, in the identification of roles and in the elaboration of business process.
Service modeling includes also the steps related to the elaboration of hyperconcepts and informational kernel [1].

The methodological approach is described below with a process model.
It intends to support the work of the service architects or method engineers which are leading the service engineering, the validation of the constraints and the services compliance analysis. We use BPMN to describe the process model.

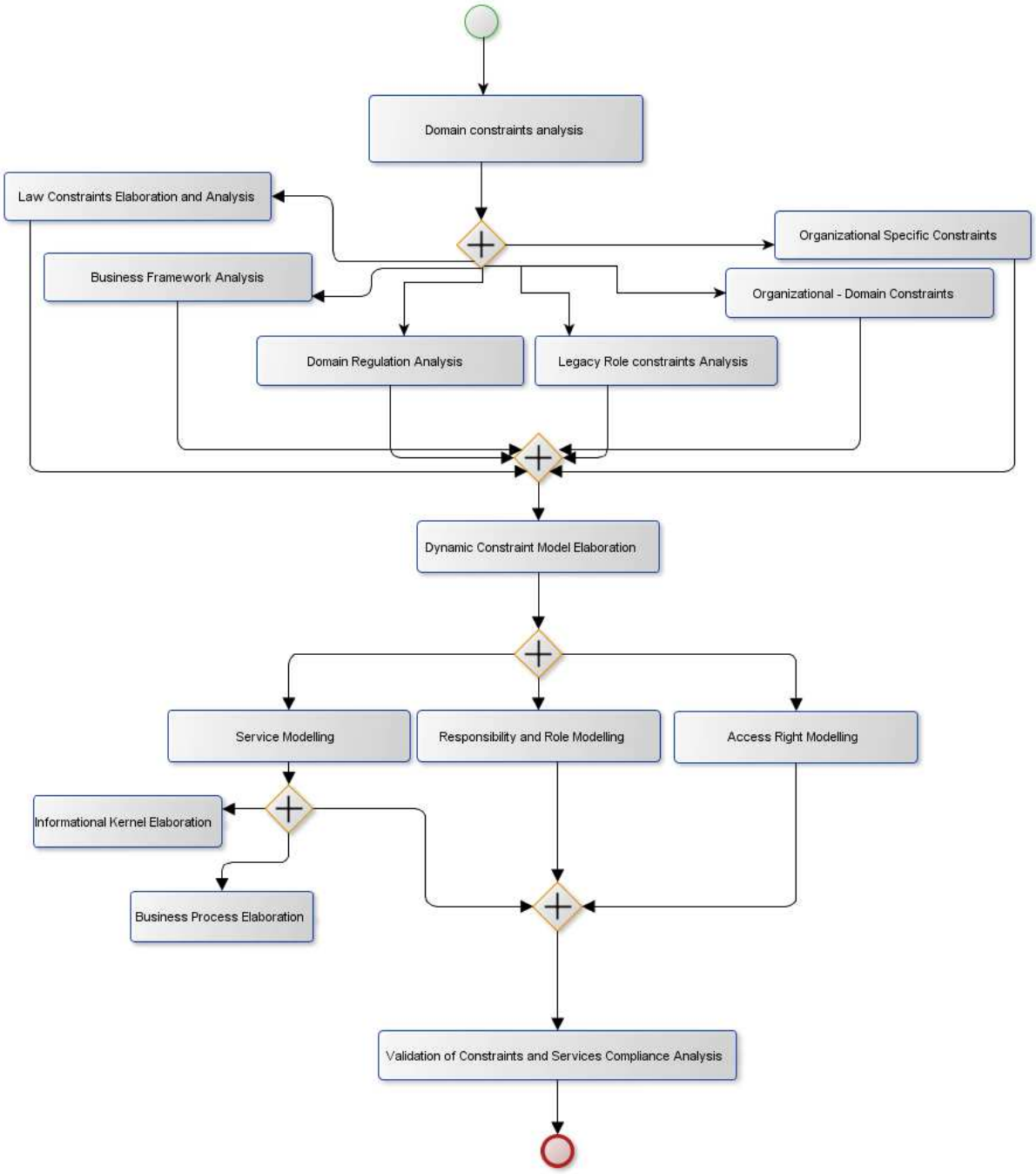

Figure 5. The process model of the proposed methodological approach

All the constraints associated to services must be identified, formalized and integrated in the business information system.

Parallel to those tasks, responsibility must be modeled for the employee involved in the task. All of those responsibilities, according to corporate rules, are gathered, afterwards, in business roles according to the organizational context. At the same time, those responsibilities are exploited, within a security perspective, to engineer the access rights needed by the employees on the services.

In accordance with this service specification activity, a complementary analysis must be lead related to the validation of the constraints having an impact on the service compliance analysis.

5 USAGE SCENARIO / CASE STUDY IN LUXEMBOURG MUNICIPAL HOSPITAL

This example is structured as follows: Firstly, we present the context and the objective of the scenario, then we engineer a service dedicated to Give access to the patients' records, finally, we analyze the compliance offered through the service when it is used by three distinct organizations. Secondly, we design the constraint model that influences the service model based on law/legal constraints on the first hand and based on the organizational constraints on the other hand.

1. Definition of the service

1.1 Context and objectives of the case study

The context of the case study, as illustrated on Figure 6, is the sharing of medical information between medical institutes from the same region, ie: the Hospitals, the National agency for statistics and the Insurance Companies. The complete case study has been presented in [1]. This case study has been realized between January 2011 and February 2012, to the rhythm of one meeting a month. During those meetings, we have collected information, we have interviewed employees and managers form the hospitals and we have validated the collected information during dedicated workshops. In this chapter, we recall the context of the case study presented in [1] and we complete it according to the constraint dimension.

At a regional layer, the healthcare institutions need to share information about the inhabitants of the region. Therefore a service is elaborated in order to share the patients' records. In order to define a service overlap (in the sense of a service that may be accessed by the 3 professional institutions in the meantime and considering the business rules), we highlight, firstly, how the Give access to the patient's record service can be specified as described previously, and, secondly, how it can be used, in compliancy with the business rules, in order to strengthen the compliancy in the usage of the services by the different actors involved.

In hospitals, doctors are often requested to delegate part of their activities to a team. This delegation is constrained by rules that are (1) dictated and at the discretion of the healthcare institute regarding the delegation process and (2) regulated by national framework, in order to fix the final accountability of the regular doctor (legally responsible doctor) attached to a patient. In practice, this delegation is very sensitive since, if the doctor has automatically access to the patient's record, the access for the rest of the team is more unstable.

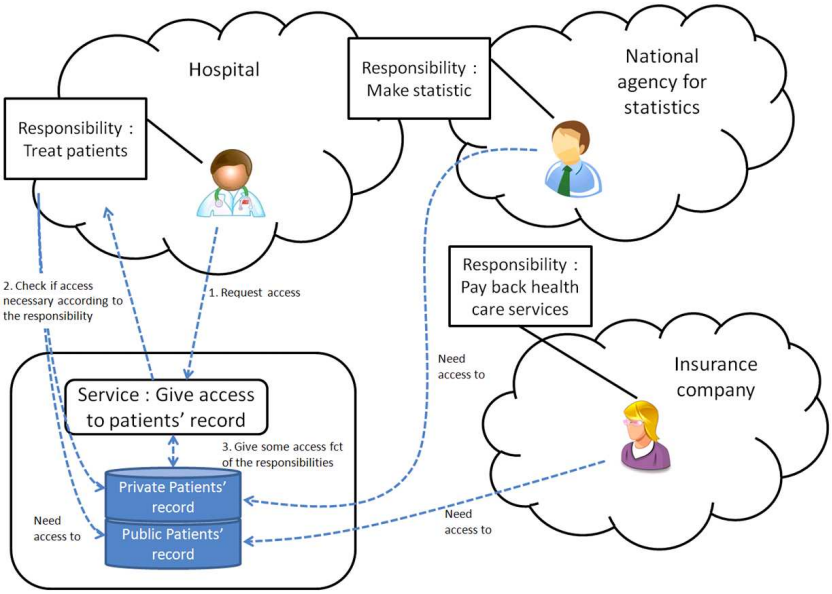

Figure 6. The context of the case study (Extracted from [1])

In this example, the added value of the service stays in the provisioning of the access rights to the right institution. Indeed, at the patient's record level, some part of the information is considered public like for instance the National healthcare ID, the age of the patient, the history of the medical acts that he has benefitted from, etc. and other information is considered private. This is the case for instance of blood analyses, serology report (eg.: HIV+), lab results, resume as the health disease and others illnesses the patient suffers, etc. Depending on the private or public character of the information, business rules constraint the access to different types of actors. The medical staff of the hospital institution is allowed to access all the information. This is justified because, on one hand, they need access to the complete history of the medical data related to the patient in order to provide care and perform medical acts, and, on the other hand, they also need access to information required for the invoicing department, including the National healthcare ID, the insurance company, etc. The insurance company only needs access to the public Patients' record in order to pay back the patient for medical acts. The National agency for statistics only needs access to the private Patient's record in order to analyze the evolution of the pathology at the regional layer. They may not access the Public Patients' record so they will not be able to retrieve the links between the patients (personally identified) and their private data.
In the example, we focus our attention on the responsibility of the doctors. In a hospital, the doctors are responsible for treating the patients. Therefore they need the capability to realize medical acts. They need the right to access the entire patient's record layer and are accountable towards the patients, the medical director of the hospital, the law and themselves (that last accountability is justified by the feeling of guilt if the patient is deceased after the treatment).

1.2 Definition of the constraint model

The definition of the constraint model is part of the definition of the services. When a service is defined, the constraint, which exists at the level of the business model, needs to be integrated through employees' responsibilities. Therefore, along the instantiation of the responsibility model, responsibilities are expressed considering those constraints. The validation of the instantiation may be achieved according to different techniques, depending on the context step of the instantiation. Eg.: During the modeling step, the model driven engineering allows to perform such kind of validation.

In order to illustrate the definition of the constraints, we will consider a delegation that happens in the hospital. For instance, when the Doctor decides to transfer the task of preparing the reporting to a nurse, he firstly asks/informs the nurse about this task she has to perform, from her side, the nurse has to accept it. In order to achieve this reporting, the nurse needs access rights to the patient records. Therefore, the Doctor requests access to the Access right manager who manages the access right service and the Nurse is assigned with these new rights. Considering this set of delegation requirements provided through a specific delegation constraint model of the hospital, we need to model the responsibility of the Doctor as well as the responsibility of the nurse according to a well-defined schema. Figure 7 represents this delegation process. Firstly, the Doctor has access to the patients' record (step 1), than he starts the delegation process to the nurse (step 2) who may or may not accept this delegation (step 3). As soon as she has acknowledged this new task, she will receive the new rights to the patients' record (step 4).

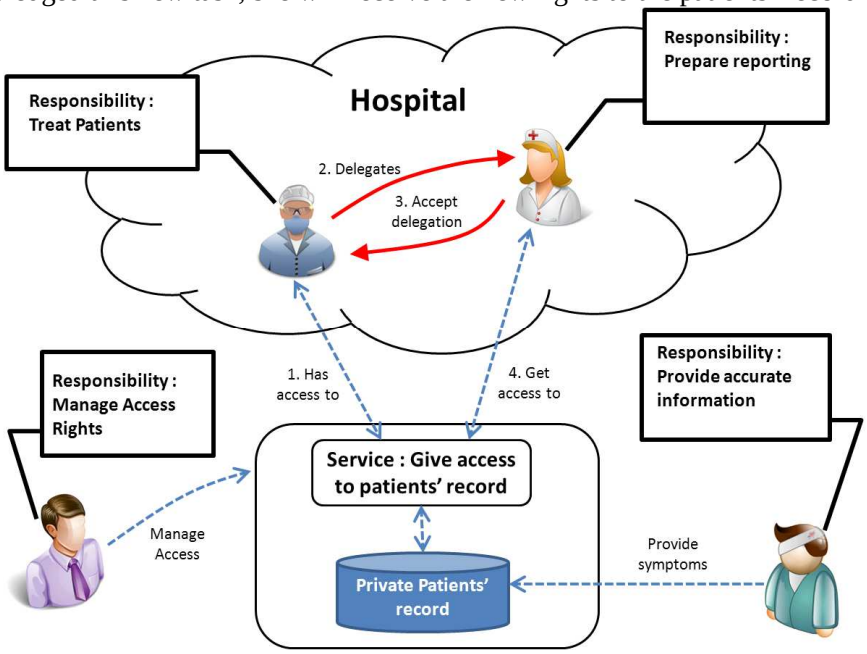

Figure 7. definition of the constraints

2. Engineering of the service

2.1 Informational Kernel Elaboration

In order to engineer and formalize the service Give access to the patient's record, we first need to specify the information system that is associated to the service. This information system is specified according to the organizational constraints that apply on the service.

In our example, the organizational constraints are different depending on whether we address confidential data or public data. Therefore, we need to create two new hyperconcepts. The first one, named Patient's record, is composed of the concept Patient that represents the human for which data exists in the database which is accessed by the service (see Figure 6). The concept Patient is associated to the concept Record which is composed of private and public data. These private and public data are associated with the concept Information system. The second hyperconcept that we create is the hyperconcept of confidentiality level. That hyperconcept results in the association of data that concerns a patient, which is accessed by a role or by an actor assigned with precise responsibilities. The concept Patient exists in both new hyperconcepts and is equivalent. The concept data exists in the information system layer, the concept role exists at the organizational layer and the concepts actor and responsibility in the responsibility

dimension. By defining that hyperconcept, we define the semantic of the confidentiality that vary depending on the type of data, type of actor and role that accesses it, type of responsibility and type of patient. For instance, the data serology analysis is confidential except for the doctors that have the responsibility to treat the patient named John or is partially available for the insurer who has a responsibility to pay back the medical act of John.
Finally, the hyperconcept of delegation is also created. This delegation is also an organizational artifact that is associated to the doctor, the doctor's responsibility, the patient, and the team.

2.2 Business Process Elaboration

Next, we have to specify the business processes which realizes and which operates the services. That specification is performed at the organizational layer which is concerned by the service and which influences the service specification. In our example, in order to have the service Give access to the patient's record operated, we have to specify the business processes that support the service as well as the business activities that complete the business processes. We consider two types of business processes. The business processes that realize the service and the business process that use the service.

2.2.1 The business process that realizes the service

In order to give access to the patient's record, the most significant process that we depict is the process that validates the compliance between the business rules and the requests issued by the different actors and the different roles. That process is composed of four business activities. The first one is the activity to receive the request, the second activity is the activity to check the compliance, the third activity is the activity to decide whether or not the access is given to the medical record and the last activity is really the provisioning of the access right. Each of these activities is associated to one or more business role(s) which objective is to realize the activity. In that case of the analysis of that process, we acknowledge that the role is mostly played by software agents that use algorithms in order to retrieve the access right query, to analyze the compliancy according to different attributes such as the business rules, to make the decision and to provide the rights.

2.2.2 The business process that operates the service

The service Give access to the patient's record is used by three types of stakeholders: the Hospital, the Statistics institute and Insurance Company. Each stakeholder needs to have access to the patient's records, in order to perform their own business processes and business activities. Let's take the example of the business process related to the treatment of the patients at the Hospital. That business process is composed of four business activities: The first one is Ask access to the patient's record, the second is Diagnose the patient's problems, the third is give drugs and perform a medical act, and the last one is Prepare reporting. In our case, all of the four activities are assigned to the business role of the Doctors.

2.2.3 The business process that manage the delegation

The service related to the treatment of the patient includes the task Prepare reporting and is assigned to the role Doctor. The constraint models apply to this task and two constraints are applicable. The first one is at the national level and required the role Doctor to always be accountable of all tasks related to the treatment of the patient. However, this law does not precise who must really perform the reporting. At the hospital internal functioning rule level, it is agreed that the doctor delegates this task to one of its subaltern under the condition that he provides this latter with the needed required information firstly and that he keeps the accountability of the rapport secondly. This second constraint is required to be compliant with the legal constraint. To be accountable of the reporting, the doctor needs: (1) to continually have access to the reports and (2) to have the possibility to check and validate the reports

before sending it in production or in archiving. Therefore, the process is structured in 4 tasks: (a) delegate the task, (b) ask for access rights for the subordinate, (3) monitor subordinate reporting and (d) validate the reporting. Specific access rights are afterwards assigned based on each task.

2.3 Responsibility Dimension Elaboration

The responsibility dimension is considered, in our product model, as the pivot that permits the alignment between the organizational layer and the information layer. Indeed, as we have previously advocated, the concept of responsibility is composed of the accountabilities to perform obligation on a business activity and it specifies, at the same time, the required rights and the. Concerning the task to ask access to the patient's record, two responsibilities exist. The first responsibility is the responsibility of making the request to the service provider. This responsibility is assigned to the doctor's assistant that requires therefore the ability to use the patient's record management system and the right to read the patient's record. It is composed of an accountability to do the request and is under the responsibility of the doctor that performs the query. The second responsibility is to decide what information from the patient's record is necessary in order to treat the patient and ask the assistant to retrieve that information. This responsibility requires a medical education and the right to make requests to the assistant. The accountability of the doctor is due to four stakeholders as explained previously.

CONCLUSION

In this chapter we discussed the issue of the definition of the constraints associated to services and the issue related to the management of access rights needed to use and exploit services. We thus proposed a process model to support the proposed approach and we discussed it in the context of the healthcare domain. The process model illustrates the main tasks in order to validate the constraints and to analyze the compliance of services.

Our future ambition is to formalize the complete set of guidelines of our approach for the validation of the constraints and the description of the impact of their evolution on different services. We continue to work on the usage-based validation of the proposed approach and we intent to define a prototype to validate the applicability, modularity and usefulness of the proposed model when it is instantiated through real situations.

REFERENCES

[1] Khadraoui A., Feltus C., Service Specification and Service Compliance: How to Consider the Responsibility Dimension?, *Journal of Service Science Research* (2012) 4:123-142, DOI 10.1007/s12927-012-0005-2.

[2] Feltus C., Petit M., Dubois E., Strengthening Employee's Responsibility to Enhance Governance of IT - COBIT RACI Chart Case Study, *The 1st ACM Workshop on Information Security Governance (ACM WISG 2009) held in conjunction with the 16th ACM Conference on Computer and Communications Security (ACM CCS 2009)*, Chicago, Illinois, USA.

[3] Feltus C., Khadraoui A., Yurchyshyna A., Léonard M., Dubois E., Responsibility aspects in service engineering for e-Government, *Interoperability for Enterprise Systems and Applications conference (I-ESA'12) Workshop Service Science and the Next Wave in Enterprise Interoperability*, Valencia, Spain.

[4] Feltus C., Dubois E., Proper E., Band I., Petit M., Enhancing the ArchiMate® Standard with a Responsibility Modeling Language for Access Rights Management, *5th ACM International Conference on Security of Information and Networks (ACM SIN 2012)*, Jaipur, Rajastan, India.

[5] Petit M., Feltus C., Vernadat F., Enterprise Architecture Enhanced with Responsibility to Manage Access Right - Case Study in an EU Institution, 5th IFIP WG8.1 Working Conference on the Practice of Enterprise Modeling (PoEM 2012), Rostock, Germany, collection Lecture Notes in Business Information Processing, volume 0134, pp. 132-147

[6] Ravi Sandhu, Transaction Control Expressions for Separation of Duties, ACSAC 1988.

[7] John C. John, Shamik Sural, Vijayalakshmi Atluri, Jaideep Vaidya: Role Mining under Role-Usage Cardinality Constraint. SEC 2012: 150-161

[8] Ezedin Barka and Ravi Sandhu. Framework for Role-Based Delegation Models, Proc. 16th Annual Computer Security Applications Conference, New Orleans, Louisiana, Dec. 11-15, 2000, pages 168-176.

[9] Xinwen Zhang, Sejong Oh and Ravi Sandhu, PBDM: A Flexible Delegation Model in RBAC, SACMAT 2003.