An Agent-based Framework for Identity Management: The Unsuspected Relation with ISO/IEC 15504

Gateau, Benjamin; Feltus, Christophe; Aubert, Jocelyn; Incoul, Christophe

Published in:
Proceedings of International Conference on Research Challenges in Information Science (RCIS), Marrakech, Morocco

DOI:
10.1109/RCIS.2008.4632091

Publication date:
2008

Document Version
Early version, also known as pre-print

An Agent-based Framework for Identity Management: The Unsuspected Relation with ISO/IEC 15504

Benjamin Gateau, Christophe Feltus, Jocelyn Aubert, Christophe Incoul

Abstract— **The generalization of open and distributed systems and the dynamics of the environment make Information Systems (IS) and, consequently, its access rights management an increasingly complex problem. Even if support for this activity appears to be well handed by current sophisticated solutions, the definition and the exploitation of an access rights management framework appropriately adapted for a company remain challenging. This statement is explained mainly by the continuous growth of the diversity of stakeholders' positions and by the criticality of the resources to protect. The SIM project, which stands for "Secure Identity Management", addresses this problem.**

The objectives of our paper are twofold. First, to make rights management align closer to business objectives by providing an innovative approach that focuses on business goals for defining access policy. The ISO/IEC 15504 process-based assessment model has been preferred for that research. Indeed, the structured framework that it offers for the description of activities allows for the establishment of meaningful links with responsibilities concepts. Secondly, to automate the deployment of policies through the company IT infrastructure's components and devices by defining a multi-agent system architecture that provides autonomy and adaptability. Free and open source components have been used for the prototyping phase.

Index Terms— **Identity Management, Multi-agent architecture, Policy Engineering, Responsibility model.**

I. Introduction

INFORMATION Systems and rights management are becoming more and more complex. This is mainly due to the generalization of open systems, heterogeneous, distributed and dynamic environments and the growth and diversity of available solutions. In that context, defining and exploiting an access control policy that addresses both the diversity of the stakeholders' statute (worker, employee or manager) and the criticality of the resources to protect (public, secret, confidential) is challenging. This challenge is then complicated due to the perpetual evolution of the organization's structure, the business strategy, the employee's responsibilities, and even the legal requirements in effect.

Solutions exist to associate rights to profiles and automatically apply those rights to all IS components and devices. These kinds of solutions (called IAM-Identity Management Solutions) are usually products with a preformatted architecture and, consequently, present difficulties in integration with the global IS solution of the company.

At a functional layer, two major problems arise when trying to deal with these existing applications. First, they are principally based on the association of stakeholders to roles following the RBAC model [1] or one of its derivations [4, 5]. In practice, and specifically in large companies, these kinds of stakeholder-roles associations are often difficult to establish because of the need to define a strict and refined number of roles. Indeed, it is uncommon to identify two employees with exactly the same job profiles. A second problem that occurs in these solutions is that the calculation of access rights is made according to the value of the asset being protected, its vulnerability, and the existing threat. IT staff are normally assigned this task and they will use existing tools issued from the risk analysis domain to complete it. These methods calculate a risk profile and propose a solution for securing the asset without systematically validating it with the asset's business owner. In that, the business owner has been given a solution without having had the possibility of optimizing the ratio "business need" / "proposed countermeasure".

Improving the way to define a more suitable IS access rights according to the business requirements is the goal of our research. We are attempting to do it by the means of policy. Policy is a concept that has already been largely discussed in scientific literature [6, 7, 8, 9]. Even if the majority of authors exploit it in the sense of a number of technical rules to be applied at a technical level [7, 8, 9], policy is also a more general concept used at the higher level of the company [6, 10, 11] (for example, Basel II [10] may be seen as imposing strategic policies for the financial sector). Whichever way policy is perceived, we would point out that no common definition of it exists yet, nor for its content [11]. However,

Article received December, 2007. This work ("An Agent-based Framework for Identity Management: The Unsuspected Relation with ISO/IEC 15504") is part of the R&D project of the CRP Henri Tudor of Luxembourg in collaboration with the University of Luxembourg". The SIM "Secure Identity Management" project was funded by the National Research Fund Luxembourg.

B. G., C. F., J. A. and C. I. are with the Centre for IT Innovation, Centre de Recherche Henri Tudor, Luxembourg, 29 Rue John F. Kennedy, L-1855 Luxembourg. Phone: +352/42.59.91-1 e-mails: {benjamin.gateau, christophe.feltus, jocelyn.aubert, christophe.incoul} @ tudor.lu.

one common component that is generally present in all definitions is the concept of "right". Right [2, 3] is defined as: privileges that a subject can hold and exercise on an object. Later in the document [2], the author characterizes this privilege as an access privilege to the object. More conceptual components of the policy exist, specifically: responsibility, obligation [2, 3, 9, 12], delegation [9], and commitment. Those components are much less systematically integrated in the definition but it has been proven that they may play an important role in refining the engineering of policy. With the desire to keep this paper didactic and based on a common understanding of the organization's artifacts, our work will be grounded on process-based organization.

At a technical layer, two observations are made: first, existing IAM solutions are usually (or generally) monolithic, proprietary and non-flexible. "Identity and access management defined" [13] explains that the complexity of integrating the components of IAM solutions will cause 60 percent of enterprises to choose product suites that are owned or licensed by, and supported through, one vendor. Secondly, the development of a Federated Identity Management (FIM) is a cornerstone concept that increases organizational cooperation by sharing each other's resources and information. However, implementing such a technology is challenging because of the difficulty in integrating heterogeneous applications – and consequently technologies - to heterogeneous organizations. To address this concern, our approach is based on the development of an open, agent-based solution. Advantages of this technology are the autonomy and the rapid and accurate adaptability according the usage constraints.

With our approach, we aim to offer a new manner to improve the way of defining a more suitable IS access rights according to the business needs and deploying these rights to their heterogeneous IS components.

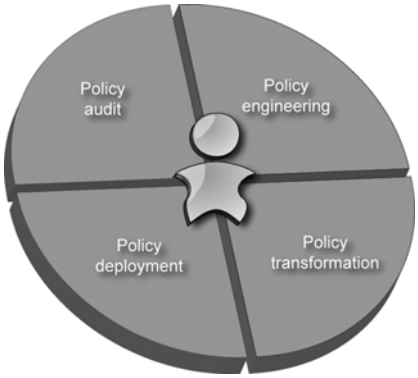


Figure 1: Identity management life cycle

As shown on Fig.1, identity management is an activity that could be achieved following a life cycle approach. First results of our research attempt to bring innovation to parts "Policy Engineering" and "Policy Deployment".

Section 2 of this paper proposes a conceptual model that integrates process concepts and responsibility components. The Section 3 presents the agent based approach for deploying policy. Section 4 introduces future work and conclusions.

II. PROCESS-ORIENTED POLICY ENGINEERING

A. Defining policy

This second section focuses on defining access control policies from the organizational structure. As explained in first section, the innovative research of this policy engineering activity is to be centred mainly on business needs. Indeed, data access is an important concept for IT security. Access policies that enforce access right must take into account both:

- the strict restriction of access for stakeholders to data ;
- the guarantee that the business goal can still be achieve in a efficient way.

To perform this policy engineering activity, we have oriented our research toward a particular type of company where process-based approaches are in use. Other frameworks also have been chosen such as the matrix approach or the pyramidal one. Future extension of this work could be done for those alternative approaches [15], even if process based approaches for formalizing the company's activity exists for a long time, a number of literature texts and norms deal with it. For example, in [16] Ruth Sara Savén describes a Business Process as a combination of a set of activities within an enterprise with a structure describing their logical order and dependence whose objective is to produce a desired result. In CEN/ENV 12204 [17] a business process is defined as a partially ordered set of enterprise activities which can be executed to realize a given objective of an enterprise or a part of an enterprise to achieve some desired end-result. Among existing process formalisms, the standard ISO 9000 [24] presents interesting perspectives in that it considers a process as a set of interrelated or interacting activities, which transforms inputs into outputs. Moreover ISO/IEC 15504 [18] confers a structural framework for describing a process and maturity model for process evaluation. Our work is based on the establishment of a link between the concepts from ISO/IEC 15504 and from the components which we will now introduce.

The project SIM aims to define policies that are a best fit for business goals and requirements. This is a basic prerequisite of business-IT alignment. These goals and requirements are translated according to ISO/IEC 15504 with process's concepts that are:

- Purposes, which describes a process;
- Outcome, which is an observable result of a process. It is an artefact, a significant change of state or the meeting of specified constraints,
- Base practice, which is an activity that, when consistently performed, contributes to achieving a specific process outcome;
- Work product, which is an artefact associated with the execution of a process. It can be input (required for outcome achievement) or output (result from outcome achievement).

Processes are observable through different outcomes and are achieved by using resources, base practices and work products.

ISO/IEC 15504 does not specifically addresses capability and accountability, which are the components of the responsibilities concepts necessary to achieve base practices. Its maturity model permits it to measure the maturity level of the processes and level 2 of this model seems adequate to deal with responsibility. Even if the standard doesn't discuss it, we have decided to orient our work according to the description of the responsibility that has been published in [15]: the Responsibility is a set of capabilities, accountabilities and commitment linked to a stakeholder that performs base practices.

- Capability, which describes the quality of having the requisite qualities or resources to achieve a task;
- Accountability, which describes the state of being answerable about the achievement of a task.
- Commitment, which is the engagement of a stakeholder to fulfil a task and the assurance he will do it.

Note that this pledge often has a character of right and an obligation to fulfil this action. Commitment may be declined under different perspectives, such as the willingness of social actors to give their energy and loyalty to social systems or an affective attachment to an organization apart from the purely instrumental worth of the relationship [19]. For James G. March and Johan P. Olsen [20], rules that manage a system exist because they work well and provide better solutions than their alternative. They also observe that peoples' moral commitment is a condition for the existence of a common interpretation of rules. According to that statement and by extrapolating "rules" to stakeholders' capabilities and accountabilities, commitment seems to be an unavoidable component.

Defining policies from business processes are obtained, in our research, by combining responsibilities and components to ISO/IEC 15504 concepts. We observe quite naturally that first, the Input Work product is a right for a stakeholder to perform an activity; it is then combined with the Capability. Secondly, the Output Work product is a stakeholder' obligation at the issue of the activity. We combine it with Accountability. Fig.2 illustrates this issue. Both responsibilities' components Capability and Accountability are strongly linked to each other [15] in that accountability of a role or a person permits us to deduce capability of another role or person and conversely a capability stems from accountability (e.g.: The capability "An engineer has access to a specific file" stems from the accountability "An engineer has to share a specific file with another engineer").

Fig.3 shows at a more global point of view of this conceptual connection between ISO/IEC 15504 and Identity Management concepts. The identity management model is composed of responsibilities associated to role, which are given to specific persons.

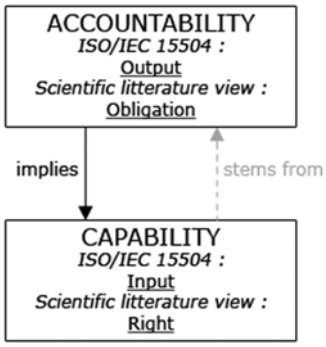


Figure 2: Relationship between accountability and capability responsibilities

- Role: which describes a role of a person in the organization;
- Person: which describes a person who interacts with the organisation and its processes.

A policy is applicable to software such as directory (LDAP, Microsoft Active Directory…) file systems (NTFS, UFS…) and hardware like firewalls or gateways.

Each responsibility is linked with a role, which describes the role of a person in the organisation (role should not be confused with the function, for example a engineer (function) can be project manager and developer (roles)).

Of course, a person can be linked to one or more roles. The role of a person permits us to define the access policy for that person; for example to grant access permission to the project management folder on the organisation's fileserver. By being linked to a role, a person has to give his/her commitment.

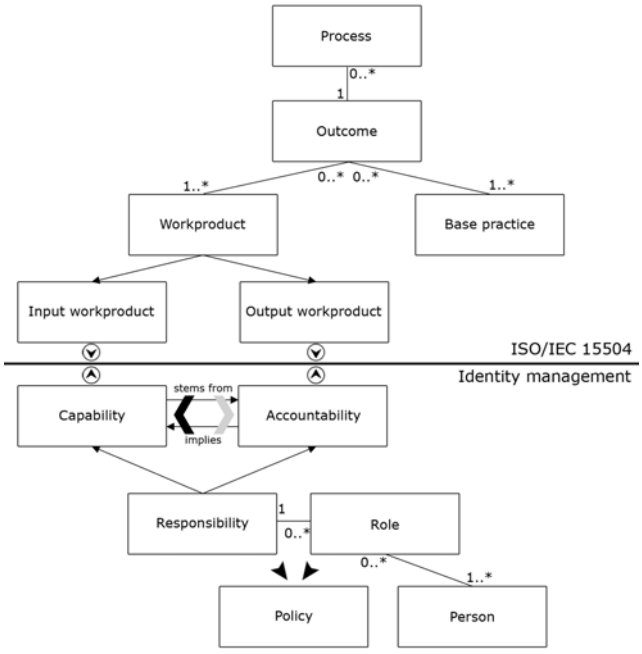


Figure 3: ISO/IEC 15504 and Identity management models

In practice, we have developing and extending modules in order to be able to define the different ISO/IEC 15504 and Identity management concepts into an open-source groupware called eGroupWare [14].

When using this application, the business owner (or the person in charge of the system) has to set up the different organisational processes as "process templates". A "process template" will describe a generic process set up in the organisation, for example the project management process, which describes all of the essential project management steps. In this kind of template-process, concepts are fully generic and responsibilities are only linked to roles.

In order to instantiate a generic process into a specific process (e.g.: project management of the SIM project), each generic concept of this process is instantiated (process, outcomes, base practices, work products, responsibilities and roles) and roles are given to specific organisation members.

With all of these parameters, SIM will be able to deduce a set of policies (hardware-applicable or not). This policy deduction will be developed in our future work.

B. Case study

To illustrate the close relation between the ISO/IEC 15504 concepts and identity management concepts we describe an example below that is a description of a part of the Process Assessment Model (PAM) of the project management process MAN3 as defined in the ISO/IEC 15504 model. Table.I shows the different concepts linked to the outcome: "*3) the tasks and resources necessary to complete the work are sized and estimated;*".

TABLE I:
MAIN CONCEPTS OF THE PROJECT MANAGEMENT PROCESS

ISO/IEC 15504-5:2006 → MAN.3 Project management	
Purpose	The purpose of the Project management process is to identify, establish, co-ordinate, and monitor the activities, tasks and resources necessary for a project to produce a product and/or service, in the context of the project's requirements and constraints.
Outcomes	… 3) the tasks and resources necessary to complete the work are sized and estimated; …
Base Practices	… MAN.3.BP4: Determine and maintain estimates for project attributes. Define and maintain baselines for project attributes. [Outcome: 2,3] MAN.3.BP5: Define project activities and tasks. Identify project activities and tasks according to defined project life cycle, and define dependencies between them. [Outcome: 3] …
Workproducts inputs	… 03-06 Process performance data [Outcome: 3,7] 08-12 Project plan [Outcome: 3, 6, 7] 10-01 Life cycle model [Outcome: 1, 3, 4, 5] 14-06 Schedule [Outcome: 1, 3] …
Workproducts output	… 08-12 Project plan [Outcome: 1, 2, 3, 4, 5] 14-06 Schedule [Outcome: 5] …

In the example detailed in Fig.4, we assume that each person is responsible of an outcome and has accepted this mission (*the commitment*). For example, the Outcome's responsible (OR) 3, to fully realise the activity, must have the *capability* (the right) to access to the "Process performance data", "Project plan", "Life cycle model" and "Schedule" resources. These elements are defined and linked to the *Input Workproducts* in the process definition.

The "schedule" capabilities for the OR3 generate obligations for another resource in the organisation. For example, OR3 has the obligation to provide the capabilities to OR3 on "Input Workproducts". In our case, it can be translated by a validation of an authorisation request (induced by this "schedule" capability).

For the "project plan", OR3 has, at the same time, a capability, but has also an obligation to participate at the elaboration of this output work product. In the same idea, OR1 and OR5 have also accountabilities on the "project plan".

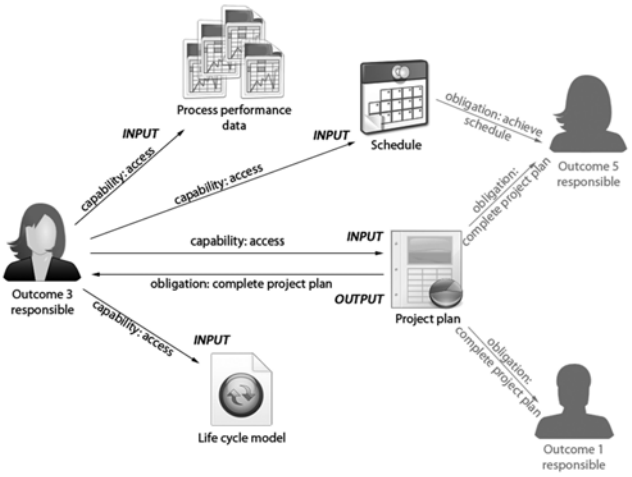
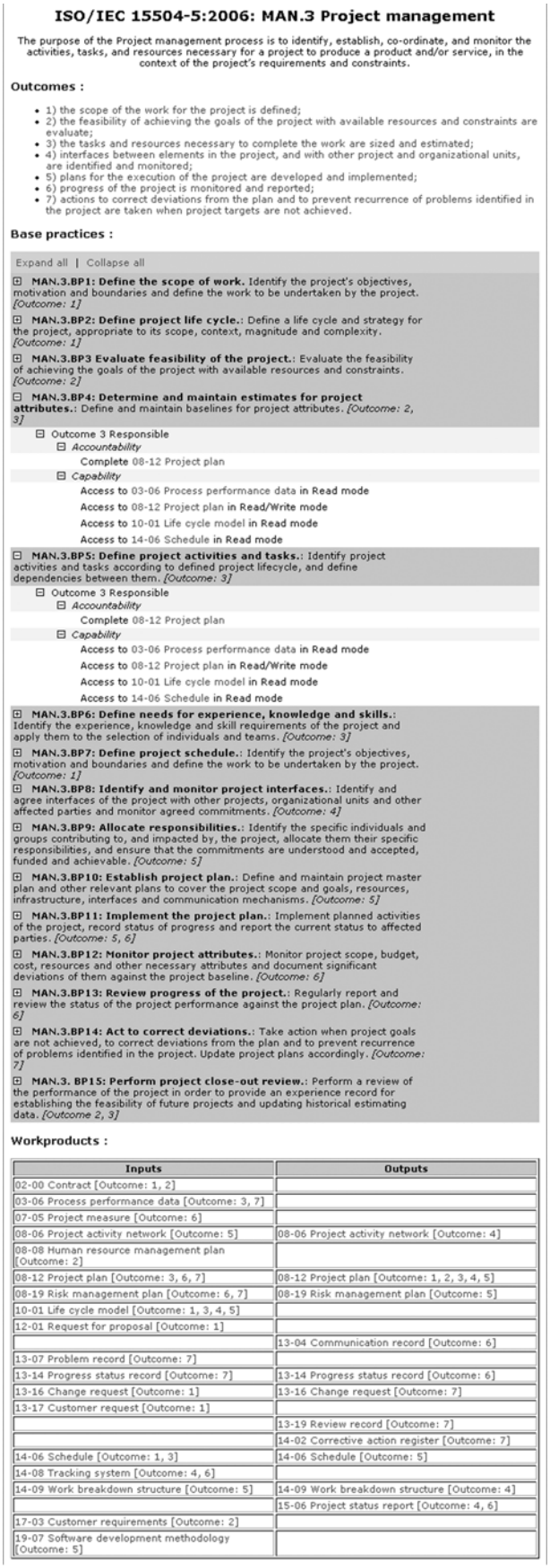


Figure 4: Responsibility decomposition of the outcome 3

In practice, these concepts are entered into the tool via eGroupWare-based modules (Process, Outcomes, Base practices and Work products). Each module permits us to link concepts to others; thus outcomes are linked to processes, and base practices and work products are linked to outcomes. The first step, as described above, is to enter the generic concepts that correspond to a generic description of a process. Once this step is realized, via the SIM module, it becomes possible to have a process cartography showing a process and its purpose, the linked outcomes, and relative base practices and work products.

Fig.5 represents the cartography of the whole process of ISO/IEC 15504-5:2006: MAN.3 Project management, with the concepts of responsibilities generated by SIM. These concepts will be called generic concepts, as the represented process is a "generic" process, responsibilities on different base practices are defined for roles.



ISO/IEC 15504-5:2006: MAN.3 Project management

The purpose of the Project management process is to identify, establish, co-ordinate, and monitor the activities, tasks, and resources necessary for a project to produce a product and/or service, in the context of the project's requirements and constraints.

Outcomes :

- 1) the scope of the work for the project is defined;
- 2) the feasibility of achieving the goals of the project with available resources and constraints are evaluate;
- 3) the tasks and resources necessary to complete the work are sized and estimated;
- 4) interfaces between elements in the project, and with other project and organizational units, are identified and monitored;
- 5) plans for the execution of the project are developed and implemented;
- 6) progress of the project is monitored and reported;
- 7) actions to correct deviations from the plan and to prevent recurrence of problems identified in the project are taken when project targets are not achieved.

Base practices :

Expand all | Collapse all

MAN.3.BP1: Define the scope of work. Identify the project's objectives, motivation and boundaries and define the work to be undertaken by the project. *[Outcome: 1]*

MAN.3.BP2: Define project life cycle.: Define a life cycle and strategy for the project, appropriate to its scope, context, magnitude and complexity. *[Outcome: 1]*

MAN.3.BP3 Evaluate feasibility of the project.: Evaluate the feasibility of achieving the goals of the project with available resources and constraints. *[Outcome: 2]*

MAN.3.BP4: Determine and maintain estimates for project attributes.: Define and maintain baselines for project attributes. *[Outcome: 2, 3]*

- Outcome 3 Responsible
  - *Accountability*
    - Complete 08-12 Project plan
  - *Capability*
    - Access to 03-06 Process performance data in Read mode
    - Access to 08-12 Project plan in Read/Write mode
    - Access to 10-01 Life cycle model in Read mode
    - Access to 14-06 Schedule in Read mode

MAN.3.BP5: Define project activities and tasks.: Identify project activities and tasks according to defined project lifecycle, and define dependencies between them. *[Outcome: 3]*

- Outcome 3 Responsible
  - *Accountability*
    - Complete 08-12 Project plan
  - *Capability*
    - Access to 03-06 Process performance data in Read mode
    - Access to 08-12 Project plan in Read/Write mode
    - Access to 10-01 Life cycle model in Read mode
    - Access to 14-06 Schedule in Read mode

MAN.3.BP6: Define needs for experience, knowledge and skills.: Identify the experience, knowledge and skill requirements of the project and apply them to the selection of individuals and teams. *[Outcome: 3]*

MAN.3.BP7: Define project schedule.: Identify the project's objectives, motivation and boundaries and define the work to be undertaken by the project. *[Outcome: 1]*

MAN.3.BP8: Identify and monitor project interfaces.: Identify and agree interfaces of the project with other projects, organizational units and other affected parties and monitor agreed commitments. *[Outcome: 4]*

MAN.3.BP9: Allocate responsibilities.: Identify the specific individuals and groups contributing to, and impacted by, the project, allocate them their specific responsibilities, and ensure that the commitments are understood and accepted, funded and achievable. *[Outcome: 5]*

MAN.3.BP10: Establish project plan.: Define and maintain project master plan and other relevant plans to cover the project scope and goals, resources, infrastructure, interfaces and communication mechanisms. *[Outcome: 5]*

MAN.3.BP11: Implement the project plan.: Implement planned activities of the project, record status of progress and report the current status to affected parties. *[Outcome: 5, 6]*

MAN.3.BP12: Monitor project attributes.: Monitor project scope, budget, cost, resources and other necessary attributes and document significant deviations of them against the project baseline. *[Outcome: 6]*

MAN.3.BP13: Review progress of the project.: Regularly report and review the status of the project performance against the project plan. *[Outcome: 6]*

MAN.3.BP14: Act to correct deviations.: Take action when project goals are not achieved, to correct deviations from the plan and to prevent recurrence of problems identified in the project. Update project plans accordingly. *[Outcome: 7]*

MAN.3. BP15: Perform project close-out review.: Perform a review of the performance of the project in order to provide an experience record for establishing the feasibility of future projects and updating historical estimating data. *[Outcome 2, 3]*

Workproducts :

Inputs	Outputs
02-00 Contract [Outcome: 1, 2]	
03-06 Process performance data [Outcome: 3, 7]	
07-05 Project measure [Outcome: 6]	
08-06 Project activity network [Outcome: 5]	08-06 Project activity network [Outcome: 4]
08-08 Human resource management plan [Outcome: 2]	
08-12 Project plan [Outcome: 3, 6, 7]	08-12 Project plan [Outcome: 1, 2, 3, 4, 5]
08-19 Risk management plan [Outcome: 6, 7]	08-19 Risk management plan [Outcome: 5]
10-01 Life cycle model [Outcome: 1, 3, 4, 5]	
12-01 Request for proposal [Outcome: 1]	
	13-04 Communication record [Outcome: 6]
13-07 Problem record [Outcome: 7]	
13-14 Progress status record [Outcome: 7]	13-14 Progress status record [Outcome: 6]
13-16 Change request [Outcome: 1]	13-16 Change request [Outcome: 7]
13-17 Customer request [Outcome: 1]	
	13-19 Review record [Outcome: 7]
	14-02 Corrective action register [Outcome: 7]
14-06 Schedule [Outcome: 1, 3]	14-06 Schedule [Outcome: 5]
14-08 Tracking system [Outcome: 4, 6]	
14-09 Work breakdown structure [Outcome: 5]	14-09 Work breakdown structure [Outcome: 4]
	15-06 Project status report [Outcome: 4, 6]
17-03 Customer requirements [Outcome: 2]	
19-07 Software development methodology [Outcome: 5]	

Figure 5: SIM module "Process cartography"

For each role, two kinds of responsibility are defined: capability and accountability. These responsibilities describe the role's rights and obligations for a given base practice. Fig.6 and Fig.7 show how responsibilities are entered. A capability is assigned to a role and needs an action, a resource and a mode (e.g.: [OR3] Outcome 3 responsible has this capability: access to 14-06 Schedule in read mode).

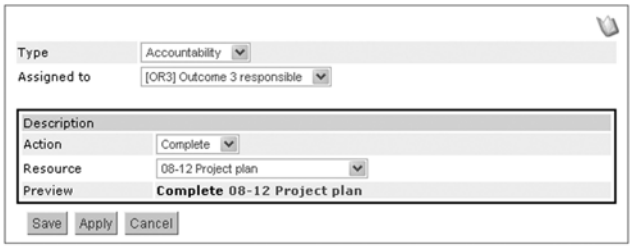


Figure 6: Capability details form

Accountability is assigned to a role and defined by an action and a resource (e.g.: [OR3] Outcome 3 responsible has this accountability: complete 08-12 Project plan). An accountability can create inherent capabilities; in order to complete an action, it is sometimes necessary to have access to something. In the case study example, the accountability complete 08-12 Project plan causes the capability Access to 08-12 Project in write mode; and it will be necessary to have permission to write to the file in order to be complete.

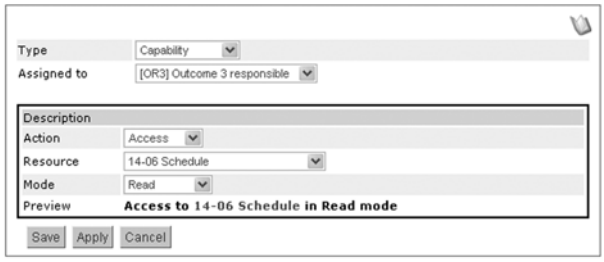


Figure 7: Accountability details form

From the model we defined, it's possible to generate generic policies that use roles in order to obtain enforceable policies and a transformation from business model to XACML [25] is done. XACML stands for eXtensible Access Control Markup Language. It's a declarative access control policy language implemented in XML and a processing model describing how to interpret the policies. The latest version 2.0 [26] was ratified by OASIS standards organization [27] on 1 February 2005; XACML 3.0 standard is not finalized yet. For this project, only the policies declaration part of XACML is used in order to store and disseminate policies through the system. A policy obtained from a generic process would not be directly applicable because it concerns roles, not physical persons. Using this generic process, it's possible to instantiate a specific process: a project management process. For example: the project management of the SIM project. In this instantiate process, roles are assigned to physical persons. In this example, Pierre Durand (defined into SIM using appropriate module: Addressbook) is assigned to the role OR3.

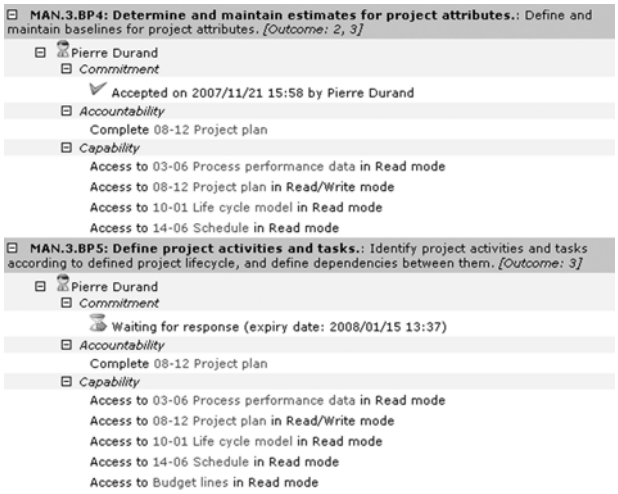


Figure 8: Instantiated responsibilities details

Fig.8 shows how responsibilities are assigned to a person (here: Pierre Durand). The responsibility of Pierre Durand is composed by accountabilities and capabilities described by the generic process model and some accountabilities and capabilities are added in order to customize the model to the needs (for example the capability Access to Budget Lines in Read mode). Knowing his capabilities and accountabilities, he can commit himself to realize a defined task.

The commitment means that Pierre Durand has accepted his responsibility according to the capabilities and accountabilities. Consequently it becomes possible to generate specific policies (specific standings for enforceable policies). The capabilities will be turned into XACML policies. From the example above, the capability "Access to 14-06 Schedule in Read mode" will be changed into XACML policy (Fig.9). Pierre Durand (subject) has to obtain read right (action) access on a resource called 14-06 Schedule (resource). Subject, actions and resources details are stored on a database. In this example, we assume that Pierre Durand's addressbook table ID (contact_id) is 42.

```
<Target>
  <Subjects>
    <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        42
      </AttributeValue>
      <SubjectAttributeDesignator AttributeId="contact_id"
        DataType="http://www.w3.org/2001/XMLSchema#string"
        MustBePresent="true"/>
    </SubjectMatch>
  </Subjects>

  <Actions>
    <Action>
      <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
          read
        </AttributeValue>
        <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
          AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"/>
      </ActionMatch>
    </Action>
  </Actions>

  <Resources>
    <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        14-06 Schedule
      </AttributeValue>
      <ResourceAttributeDesignator
        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
        DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </ResourceMatch>
  </Resources>
</Target>
```

Figure 9: XACML policy example

Using all of the defined capabilities of each instantiated process, SIM will be able to generate a full set of policies, which will be transferred to the agent-based policy deployment.

III. AGENT-BASED POLICY DEPLOYMENT

We need a means to apply policies in terms of specific concrete rules. The communication between a component managing the policies resulting in process-oriented policy engineering and the devices which must apply concrete rules should be provided by a standardized protocol such as SNMP [30], COPS [28] or NETCONF [29]. Another solution is to use multi-agent based communications.

SNMP is a simple network management protocol designed by the IETF (Internet Engineering Task Force). An SNMP-managed network consists of three key components: (i) a network management station (NMS) executing applications that monitor and control managed devices, (ii) the managed devices i.e. network nodes that we want to manage and (iii) SNMP agents which are network-management software modules residing in managed devices.

COPS is a signaling protocol designed by the IETF for exchanging policy information between a policy server (Policy Decision Point or PDP) and its clients (Policy Enforcement Points or PEP). It is a simple query and response protocol that can be used to send configuration requests and return policy decisions to enforce.

NETCONF is a network management protocol standardized by the IETF. The NETCONF protocol provides mechanisms to install, manipulate, and delete the configuration of network devices. It also can perform some monitoring functions. It uses an Extensible Markup Language (XML) based data encoding for the configuration data as well as the protocol messages. The NETCONF protocol operations are realized on top of a simple Remote Procedure Call (RPC) layer.

If we take the terms defined by COPS, these protocols could be used to send messages between a PDP and some PEP. These protocols are secured and permit a certain quality of service. But they don't specify how a PEP transforms an abstract policy sent by the PDP into a concrete rule. These solutions neither define architecture and functions of PDP and PEP. These components must not only send messages but also "work together" to apply concrete rules on devices. That's why we think that the use of a Multi-Agent System (MAS) is a solution because it provides autonomous entities that can be collaborative. A Multi-Agent System is composed of several agents, capable of a mutual interaction which can be in the form of message passing or the production of changes in their common environment [21]. Agents are pro-active, reactive and socially autonomous entities able to exhibit organized activity, in order to meet their designed objectives, by eventually interacting with users. Agents are collaborative by being able to commit themselves to the society or/and another agent [22]. So, if we consider that each technical module (firewall, fileserver, LDAP directory, etc.) is interfaced with

an agent, all agents will collaborate in order to apply a set of common policies.

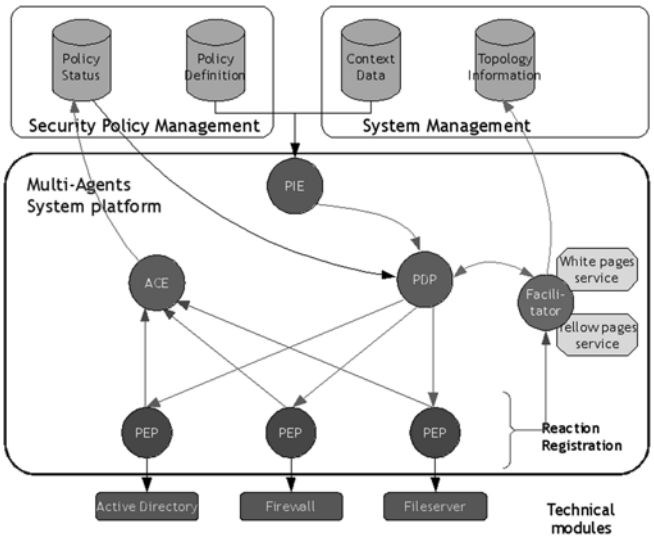


Figure 10: Multi-Agent System framework

We propose a Multi-Agent System gathering three types of agents to build the SIM's technical architecture as shown in Fig.10. Each device (technical module) is interfaced with an agent called PEP for Policy Enforcement Point. The PEP communicates with an agent called PDP (for Policy Decision Point) whose goal is to retrieve PEP agents and distributing policy to be applied. At last, the PIE agent (Policy Instantiation Engine) interfaces with the policy base in order to be aware of new policies to apply. We give main functionalities of each of the kinds of agents in the following sections.

A. Policy Instantiation Engine

This is the interface between the policies and the agents, between the transformation of the business process definition and its deployment. PIE agents detect when new policies are available and must be applied or when some policies have been modified or deleted. At this moment, it sends requests to add, modify or delete some policies to the PDP. For that, it must be able to make difference between new and previous organisation configuration by producing messages asking to add, modify or delete policies.

B. Policy Decision Point

The PDP's architecture is shown in Fig.11. There are two main modules: the policy analysis and the component configuration mapper. The policy analysis module has to perform a variety of validation checks.

First, it verifies the syntax of the policy specification provided by a PIE. This module will then verify that the newly received policies are consistent with current applied rules (coming from the policy status base). A set of policies will be consistent if it can be shown that no contradictory policies will ever be found in a SIM system. The user will be able to choose the system behavior if a conflict is detected. For the moment, the old rules that derivate from the previous policy are canceled and the newly received policy that contradicts the applied rules.

The policy analysis module communicates with a "policy rules status" database. This database stores the newly received policies and their current status (in progress, not applicable, by-passed, enforced, removed…). In addition, the module should detect rules that cannot be enforced due to a lack of PEP. As a consequence a PDP should be aware of the different managed PEPs.

For this reason, the PDP agent is helped by a Facilitator agent. This agent manages the network topology by retrieving PEP agents according to their localisation (devices registered with an IP address or MAC address) or according to actions they could apply and their type (firewall, fileserver, etc.). For this, the Facilitator uses white pages and yellow pages services.

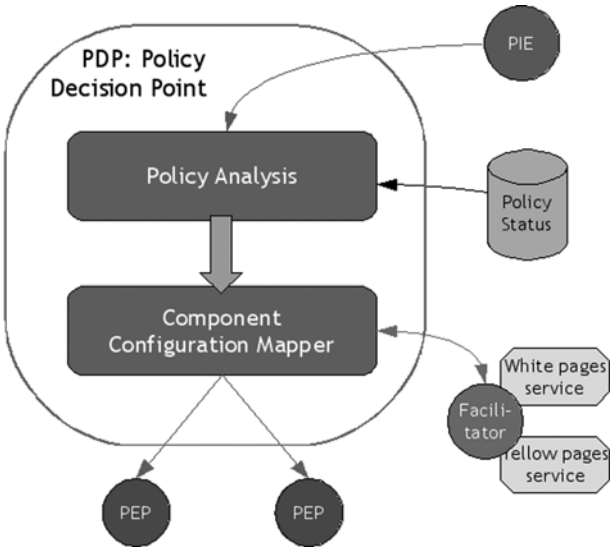


Figure 11: Policy Decision Point architecture

The Component Configuration Mapper must state in detail which kind of actions need to be taken by which kind of network devices/applications. This module receives high level policies and generates generic format policies for each type of PEP (router, firewall, IDS…). For that, it asks the Facilitator to determine what PEPs are impacted by the policies update by mapping a set of possible actions to the current network components capabilities.

If some rules are not applicable, the component configuration mapper notifies the policy analysis module. This one will update the policy rules status. Problematic rules will be passed by, and their status in the "policy status" database will change from "in progress" to "by-passed". Then the corresponding policies are sent to the concerned PEP.

C. Policy Enforcement Point

A PEP agent must manage each device that is part of SIM's technical layer. Agents are specific according to the kind of devices or the kind of services that the device offers. It is

specific in order to know how to transform policies represented in an abstract format (XACML [23] in our case) for applicable scripts or rules. Fig.12 shows the PEP's architecture. A PEP is composed of three modules which are referred to as monitoring, observation and enforcement.

The monitoring module controls the PEP actions and stores all relevant actions/events. It receives abstract policy from the PDP and chooses which action and parameters must be executed to apply the policy. Then, the enforcement module launches this local appropriate action mechanism by applying the selected script. The progress of the operations can be provided to the Observation module. This last module performs periodically, or during a script execution, measurements to evaluate the current state of the PEP. But this is also the module through which an audit could be done by sending feedback to the Audit Correlation Engine (ACE).

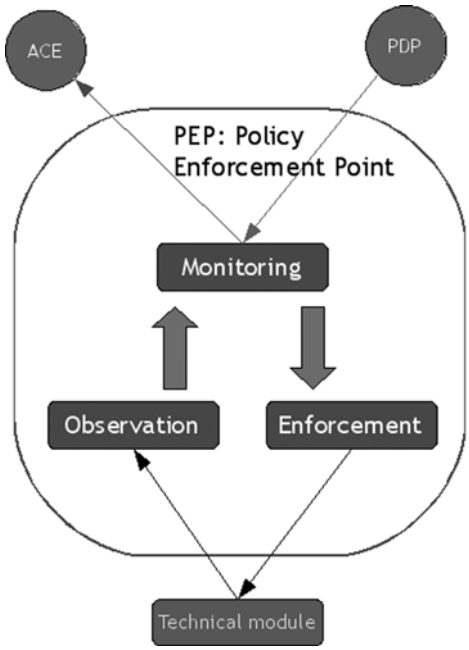


Figure 12: Policy Enforcement Point architecture

Let us take the policy example from Fig.9 permitting the user "42" to read the resource "14-06 Schedule". The PEP interfacing with a UNIX-like fileserver registered the "chmod" action. So it will construct its script to execute with elements from the policy: the permission to read will be transformed into '+r'. If we consider that user "42" is not the owner of the file, the command to execute will be "chmod a+r 14-06 Schedule"and the enforcement module of the PEP will execute it. The observation module will perform measurements and feedback information concerning the fileserver rules. In this particular case and for this resource, it will send a policy saying that all users are permitted to read the "14-06 Schedule" resource and not only the user "42".

To summarize, the use of a multi-agent system framework gives PIE, PDP and PEP the ability to cooperate and communicate between themselves in order to implements policies. It also provides flexibility, openness and heterogeneity because when we decide to add a new PEP, we just have to provide the agent able to concretely apply the policies.

IV. Conclusion and Future Work

This paper introduces the SIM approach, an innovative environment for defining and deploying policies in a heterogeneous environment. SIM facilitates the rights management by using a process approach based on business goals. This business-oriented approach is facilitated by the conjunctive use of the ISO/IEC 15504 and identity management concepts. The set of policies resulting of this engineering can be deployed using a multi-agent system. For example, agents collaborate in order to send abstract policies to each device concerned and to transform and implement them concretely on each system by executing scripts on a fileserver or adding rules for a firewall. This solution provides heterogeneity, flexibility and openness because of facilitator registering agents and the same abstract policies format used between agents. Agents deploy common rules but the administrator can modify system configurations directly.

Current and future work will focus on the enhancement of the approach in the following domains shown in Fig.1: the "Policy Audit" and in the "Policy Transformation". Concerning the "Policy Audit", in order to avoid a difference between the organisational point of view and the system configuration point of view, we plan to give agents the ability to do an audit on their system on feed-back deployed policies to compare with the policies coming from the engineering activities. Deeper work in the "Policy Transformation" will also be conducted in order to develop a policy deduction strategy from the organisational layer to the technical one.

Future works will also be concerned with the communication between agents and how to make them secure. We plan to use the JADE framework which uses the FIPA-ACL message. The main attributes are the sender, the receiver, the language and the protocol used and the content of the message. We have to choose the language and then define the protocol that the agents will follow in order to deploy a set of policies and to audit applied rules. Next, we will improve the message structure by adding certificate information as in [31] in order to fill the security gap.

Acknowledgment

SIM "Secure Identity Management" is an R&D project of the CRP Henri Tudor developed in collaboration with the « University of Luxembourg » and funded by the National Research Fund Luxembourg.

References

[1] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn and R. Chandramouli, "Proposed NIST standard for role-based access control", ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001, Pages 224-274.

[2] J. Park, R. Sandhu, “Originator control in usage control”, Policy 2002: IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, Monterey, California, U.S.A.

[3] J. Park, R. Sandhu, “Towards usage control models: beyond traditional access control”, SACMAT’02, June 3-4, 2002, California, USA.

[4] R. K. Thomas, “Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments”, RBAC '97: Proceedings of the second ACM workshop on Role-based access control, 1997.

[5] A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, and al., “Organization based access control.” IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy 2003), Lake Come, Italy, June 4-6, 2003.

[6] A. I. Antón, J. B. Earp, “Strategies for developing policies and requirements for secure electronic commerce systems”, 1st Workshop on Security and Privacy in E-Commerce at CCS2000.

[7] P. Samarati, S. De Capitani di Vimercat, « Access control: policies, models, and mechanisms », IFIP WG 1.7 Int’l School on Foundations of Security Analysis and Design (FOSAD 2000), LNCS 2171, pp. 137-196, 2001.

[8] R. Crook, D. Ince, B. Nuseibeh, “Modelling access policies using roles in requirements engineering”, Information and Software Technology 45 (2003) 979-991.

[9] N. Dulay, E. Lupu, M. Solman, N. Damianou, “A policy deployment model for the ponder language », An extended version of paper in Proc. IEEE/IFIP International Symposium on Integrated Network Management, (IM’2001), Seattle, May 2001, IEEE Press.

[10] Basel Committee on Banking Supervision, “International convergence of capital measurement and capital standards”; BIS; Basel, June 2004.

[11] C. Camerer, “Redirecting research in business policy and strategy, Strategic Management Journal, Vol.6, No. 1. (Jan. – Mar., 1985), pp. 1-15.

[12] D. Marriott and M. Sloman, "Implementation of a management agent for interpreting obligation policy", IFIP/IEEE 7th international workshop on distributed systems operations and management (DSOM), 1996.

[13] R. J. Witty, A. Allan, J. Enck, R. Wagner, "Identity and access management defined", Publication Date: 4 November 2003, Gartner Research.

[14] Official eGroupWare community website, http://www.egroupware.org, December 5, 2007.

[15] C. Feltus and A. Rifaut, “An ontology for requirements analysis of managers’ policies in Financial Institutions”, I-ESA07, 2007.

[16] R. S. Savén, Process modelling for enterprise integration: review and framework, 13th International Working Seminar on Production Economics, Igls/Innsbruck, Austria, February 18-22, 2002.

[17] CEN/ENV 12204: Advanced manufacturing technology - Systems architecture - Constructs for enterprise modelling, CEN TC 310/WG1, 1996.

[18] ISO/IEC 15504, “Information Technology – Process assessment”, (parts 1-5), 2003-2006.

[19] Md. Zabid A. Rashid, M. Sambasivan, J. Johari, “The influence of corporate culture and organisational commitment on performance”, Journal of Management Development, ISSN: 0262-1711, Vol, 22., issue 8, pp. 708 – 728.

[20] J. G. March and J. P. Olsen, The logic of Appropriateness, ARENA Working Papers WP 04/09.

[21] J-P. Briot and Y. Demazeau, “Principes et architectures des systèmes multi-agents”, Hermés-Lavoisier, 2001.

[22] N. R. Jennings and M. J. Wooldridge, “Applications of intelligent agents”, Agent Technology Foundations, Applications, and Markets, Springer-Verlag, 1998.

[23] S. Godik, T. Moses, et al, “eXtensible Access Control Markup Language (XACML) Version 1.0”, OASIS Standard, February 18th, 2003.

[24] ISO 9000:2005, Quality management systems - Fundamentals and vocabulary.

[25] eXtensible Access Control Markup Language (XACML) homepage, http://xml.coverpages.org/xacml.html, December 12, 2007.

[26] XACML 2.0 Specifications, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#XACML20, December 12, 2007.

[27] Organization for the Advancement of Structured Information Standards (OASIS) homepage, http://www.oasis-open.org/home/index.php, December 12, 2007.

[28] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry, “The COPS (Common Open Policy Service) protocol”, IETF RFC 2748, January 2000.

[29] R. Enns, “NETCONF configuration protocol”, IETF RFC 4741, december 2006.

[30] D. Harrington, R. Presuhn, B. Wijnen, “An architecture for describing Simple Network Management Protocol (SNMP) management frameworks”, IETF RFC 3411, December 2002.

[31] P. Novàak, M. Rollo, J. Hodik and T. Vlcek, “Communication security in multi-agent systems”, Multi-Agent Systems and Applications III, Lecture Notes in Computer Science 2691,pp 454-463, 2003.