SIM : an Innovative Business-Oriented Approach for a Distributed Access Management

Jocelyn Aubert, Benjamin Gateau, Christophe Incoul, Christophe Feltus
Centre for IT Innovation
Centre de Recherche Public Henri Tudor
Luxembourg-Kirchberg, Luxembourg
{jocelyn.aubert, benjamin.gateau, christophe.incoul, christophe.feltus}@tudor.lu

Abstract— **The generalization of open and distributed system and the dynamicity of the environment make the Information Systems (IS) and consequently its access right management always more complex. Even if the support of this activity appears to be well handed by current sophisticated solutions, the definition and the exploitation of an access right management framework appropriately adapted for a company remains challenging. This statement is explained mainly by the continuous grow of the diversity of stakeholders' statuses and by the criticality of the resources to protect. To face that problem, the objectives of this paper are twofold. Firstly to make right management closer with business objectives by providing an innovative approach that focus on business goals for defining access policy. The ISO/IEC 15504 process-based model organization has been preferred for that research. Indeed, the structured framework that it offers for the description of activities allows to established meaningful links with responsibilities concepts. Secondly, to automate the deployment of policies through the infrastructure's components and devices by defining a multi-agent system architecture that provides autonomy and adaptability. Free and open source components have been privileged for the prototyping phase.**

Identity management, Business IT-alignment, Policy engineering, Agent-based architecture

I. Introduction

Information Systems and right management are becoming more and more complex. This is mainly due to: firstly, the generalization of open system, heterogeneous, distributed and dynamic environment and secondly, the multiplication and the diversity of available solutions. In that context, defining and exploiting an access control policy that take care at the same time of the diversity of the stakeholders' statute (worker, employee or manager) and of the criticality of the resources to protect (public, secret, confidential) is challenging. This challenge is moreover complicated due to the perpetual evolution of the organization structure, the business strategy, the employee's responsibilities, and even due to the legal requirement in effect.

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

At a functional layer, two major problems arise when trying to deal with those existing applications. Firstly, 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 in large company, those kinds of stakeholders-roles association are often difficult to be established because of the need to define a strict and reduced enough number of roles. Indeed, it is uncommon to identify two employees with exactly the similar job profile. A second problem that occurs in those solutions is that the calculation of access right is made according to the value of the asset to protect, its vulnerability and the existing threat. IT staff is often been delegated this task and uses existing tools issued from the risk analysis domain to complete it. Those methods calculate a risk profile and propose solution for securing the asset without systematically validate it with the asset's business owner. In that, the business owner is imposed a solution without having had the possibility to optimize the ratio "business need" / "proposed countermeasure".

Improving the way of defining the more suitable IS access right according to the business needs is our research's aim. We are attempting to do it by the means of policy. Policy is a concept that has already largely been discussed in the 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 the 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). Whatever the way policy is perceived, we would highlight that no common definition of it exists yet, neither of it content [11]. However, one common component that is mostly present in all definitions is the right. In [2, 3] right is defined as: privileges that a subject can hold and exercise on an object. Further in [2], the author characterized this privilege as an access privilege to the object. More conceptual components of the policy exist, among others: responsibility, obligation [2, 3, 9, 12], delegation [9], and commitment. Those components are much less systematically integrated in the definition but it is proved that they may play an important role in fine grain engineering of policy. With the desire to keep this paper didactic and based on a common understanding of organization's artifacts, the work will be grounded on process-based organization.

At a technical layer, two observations are done: firstly, existing IAM solutions are most of the time monolithic, proprietary and non-flexible. *Identity and Access Management Defined* [25] 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 organization's cooperation by sharing each other's resources and information. However, implementing such a technology is challenging because of the difficulty to integrate heterogeneous applications - consequently technologies - to heterogeneous organizations. To face 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 context.

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

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".

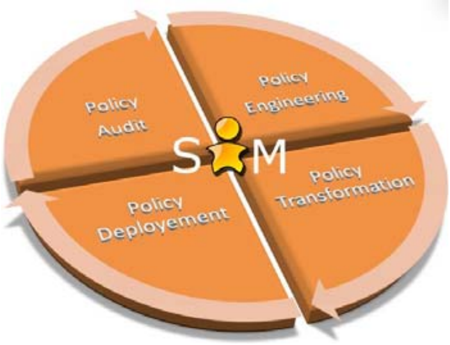

Figure 1. Identity management life cycle

The 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 introduce future work and conclude.

II. PROCESS-ORIENTED POLICY ENGINEERING

A. Methodology

This second section aims at defining access control policies from the organizational structure. As explained in first section, the innovative research of this policy engineering activity is to be centered mainly on the business needs. Indeed, data access is an important concept for IT security. Access policies that enforce access right must consequently be constructed at the same time on limiting as much as possible the access to data for stakeholders that really need it and in the certainty that necessary right for the business' purpose are guaranteed.

To perform this policy engineering activity, we have oriented our research toward a particular type of companies where process-based approaches are in use. Other frameworks should 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 [14]. Whatever process based approach for formalizing the company's activity exists for a long time. A number of literature texts and norms deal with it. For example in [15] 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 or in CEN/ENV 12204 [16] where 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 [17] confers a structural framework for describing process and a maturity model for process evaluation. Our work is based on the establishment of a link between concepts from ISO/IEC 15504 and from the responsibility's components.

The project SIM, stands for "Secure Identity Management", aims to define policy that best fit to business goals and requirements. This is a basic prerequisite of Business-IT alignment. Those goals and requirements are translated according to ISO/IEC 15504 throughout 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;
- *Workproduct*, 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 workproducts.

ISO/IEC 15504 has not for aim to clarify responsibilities' components necessary to achieve base practices. Its maturity model permit to measure the maturity level of the processes and at the level 2 of this model appear the necessity to deal with responsibility. Whatever, the standard is not talkative about that and consequently doesn't give much more information about how to deal with it. Due to that lack of information, we have decided to orient our work according to the description of the responsibility that has been published in [14]: the Responsibility is a set of capabilities, accountabilities and commitment link 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 obligation to fulfill 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 [18]. For James G. March and Johan P. Olsen [19], rules that manage a system exist because they work well and provide better solutions than their alternative and 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 process is obtained, in our research, by combining responsibilities components to ISO/IEC 15504 concepts. We observe quite naturally that firstly, the Input Workproduct is a right for a stakeholder to perform an activity; it is by the way combined with the Capability. Secondly, the Output Workproduct is a stakeholder' obligation at the issue of the activity. We combine it with Accountability. Fig. 2 illustrates that issue. Both responsibilities' components Capability and Accountability are strongly linked to each other [14] in that accountability of a role or a person permits 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").

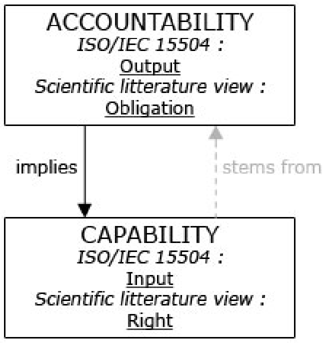

Figure 2. Relationship between accountability and capability responsibilities

Fig. 3 shows at a more global point of view 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.

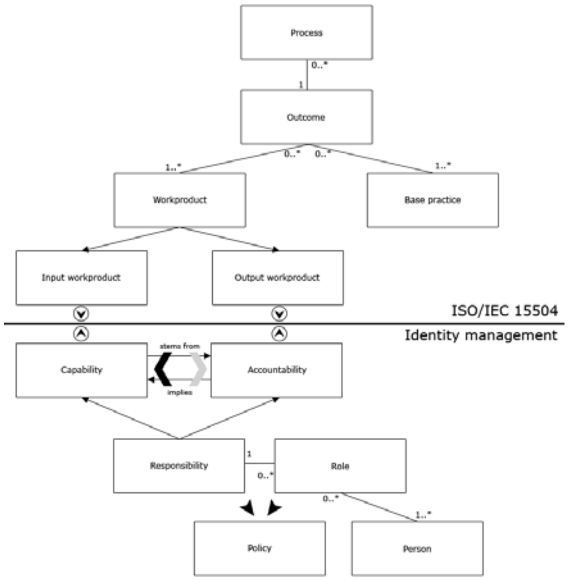

Figure 3. ISO/IEC 15504 and Identity management models

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

A policy is applicable on 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 a role of a person in the organization (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 to determinate policies on this person; for example access permission to project management folder on the organization's fileserver. For being linked to a role, a person has to give his/her commitment.

In practice, we are creating and extending modules in order to be able to define the different ISO/IEC 15504 and Identity management concepts into the open-source groupware eGroupWare [13].

When using the application, the business owner (or the person in charge to initiate the system) has to set up the different organization's processes as "process templates". A "process template" will describe a generic process setting up in the organization, for example the project management process, which describes all 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, workproducts, responsibilities and roles) and roles are given to specific organization members.

With all this 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 the 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 defined in the ISO/IEC 15504. Table 1 shows the different concepts links 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). In Fig. 4, the Outcome's responsible (OR) 3, to fully realize the outcome, must have the capability (the right) to access to the "Process Performance data", "Schedule", "Project Plan" and the "lifecycle Model" 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 organization. For example, the responsible of 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 authorization 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 workproduct. In the same idea, OR1 and OR5 have also capabilities on the "project plan".

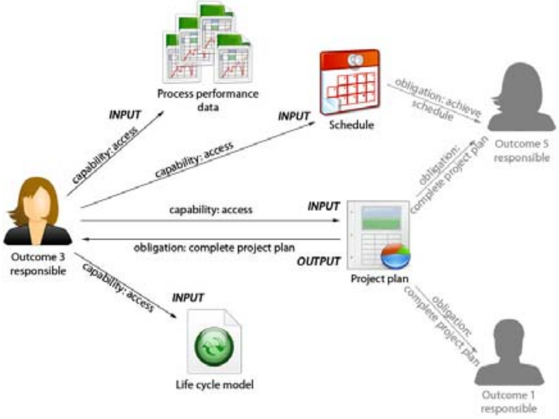

Figure 4. Responsibility decomposition of the outcome 3

III. AGENT-BASED POLICY DEPLOYMENT

We need a means to apply policies in terms of specific concrete rules. We think that Multi-Agent Systems technology is a solution because it provides autonomous entities able to be collaborative.

A. *Multi-Agent Systems definition*

A Multi-Agent System (MAS) is a system composed of several agents, capable of mutual interaction. The interaction can be in the form of message passing or producing changes in their common environment [20].

Agents are pro-active, reactive and social autonomous entities able to exhibit organized activity, in order to meet their design objectives, by eventually interacting with users. Agent is collaborative by being able to commit itself to the society or/and another agent [21].

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.

B. *SIM's technical layer framework*

A Multi-Agent Systems gathering three types of agents composes the SIM's technical architecture. Each device is interfaced with an agent called PEP for Policy Enforcement Point. The PEP communicates with an agent called PDP (for Policy Decision Point) aiming at retrieving PEP agents and distributing policy to apply. At last, the PIE agent (Policy Instantiation Engine) interfaces the policy base in order to be aware of new policies to apply. Fig. 5 represents the SIM policy enforcement architecture with the PIE, PDP and PEP.

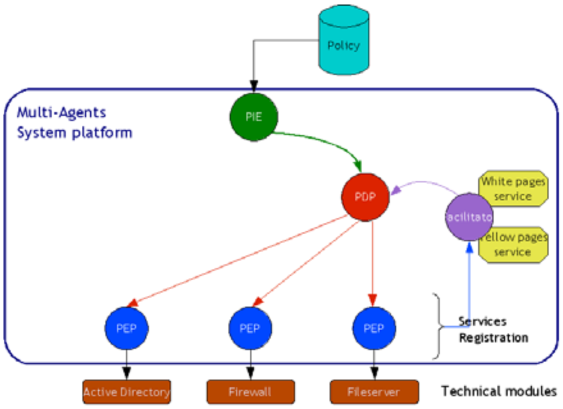

Figure 5. Multi-Agent System framework

We give main functionalities of each kind of agents in following sections.

1) *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 agent detects when new policies are available and must apply or when some policies are 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.

2) *Policy Decision Point*

The PDP agent helped by a Facilitator agent (see Fig. 5) determines which PEP agents are concerned by the policies update. This agent manages the network topology by retrieving PEP agents according to their localisation (devices registered with IP address or MAC address) or according to actions they could apply and their type (firewall, fileserver, etc.). For that the Facilitator uses white pages and yellow pages services.

Once the PDP receives requests from the PIE, it decides which PEP are concerned by the request and are able to implement policies in terms of rules or script on devices. Then, the PDP sends to the concerned PEP their corresponding policies.

3) *Policy Enforcement Point*

A PEP agent must manage each device being 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 transform policies represented in an abstract format (like XACML [22] or CIM [23] for instance) in applicable scripts or rules.

When a new device is added, its PEP has to register itself through the Facilitator in order to be retrieved in the yellow and white pages services. The registration must be done because it is on this information that the PDP based the dispatching of incoming policies to update.

When the PDP knows which devices are able to adapt the policies into their specific representation, it sends messages to PEP. The PEP transforms policies into script or rules and applies them by adding a new entry in the route table or new access right for a file.

To summarize, the use of a multi-agent system framework makes PIE, PDP and PEP able to cooperate and communicate between them 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 heterogeneous environment. SIM facilitates the right 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 the identity management concepts. The set of policies resulting of this engineering can be deployed using a multi-agent system. Agents collaborate in order to send abstract policies to each device concerned and to transform and implement them concretely on each system by executing script for a fileserver or adding rules for a firewall for instance. This solution provides heterogeneity, flexibility and openness because of facilitator registering agents and same abstract policies format used between agents. Agents deploy common rules but administrator can modify system configuration directly.

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

Acknowledgment

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

References

[1] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn and Ramaswamy 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] Jaehong Park, Ravi 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] Jaehong Park, Ravi Sandhu, "Towards Usage Control Models: Beyond Traditional Access Control", SACMAT'02, June 3-4, 2002, California, USA.

[4] Roshan 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, Y. Deswarte, A. Miège, C. Saurel et G. Trouessin, “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] Annie I. Antón, Julia 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] Robert Crook, Darrel Ince, Bashar 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] Colin 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] Official eGroupWare community website, http://www.egroupware.org, December 5, 2007.

[14] C. Feltus and A. Rifaut, “An Ontology for Requirements Analysis of Managers’Policies in Financial Institutions”, I-ESA07, 2007.

[15] Ruth Sara Savén, Process Modelling for Enterprise Integration: review and framework, 13th International Working Seminar on Production Economics, Igls/Innsbruck, Austria, February 18-22, 2002.

[16] CEN/ENV 12204: Advanced Manufacturing Technology - Systems Architecture - Constructs for Enterprise Modelling, CEN TC 310/WG1, 1996.

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

[18] Md. Zabid Abdul Rashid, Murali Sambasivan, Juliana 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.

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

[20] Jean-Pierre Briot and Yves Demazeau, Principes et architectures des systémes multi-agents, Hermés-Lavoisier, 2001.

[21] Nicholas R. Jennings and Michael J. Wooldridge, Applications of intelligent agents, Agent Technology Foundations, Applications, and Markets , Springer-Verlag, 1998.

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

[23] "Common Information Model (CIM) Policy Model White Paper Version 2.7", Distributed Management Task Force, Inc. (DMTF), June 18th, 2003.

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

[25] Identity and Access Management Defined, Roberta J. Witty, Ant Allan, John Enck, Ray Wagner, Publication Date: 4 November 2003, Gartner Research.