HYPR&A - A SECURITY MODEL FOR THE SUPPORT PROCESSES IN EGOVERNMENT

Tatyana Podgayetskaya, Wolffried Stucky
University of Karlsruhe, D-76128 Karlsruhe, Germany, {tpo,wst}@aifb.uni-karlsruhe.de

Abstract: During eGovernment processes often sensitive data are worked on. The authorization to work on or pass data on should not only of security policy certainly, but also by the technology and/or Business Process support systems (BPS Systems) to be supported. HyPR&A, hybrid process-oriented role and task security model, is a model for eGovernment organizations, which support eGovernment processes. In this article HyPR&A is developed and adapted on basis of architecture for Workflow Enactment services for BPS System

Key words: security model, workflow, information system, eGovernment.

1. INTRODUCTION

1.1 Problem definition. Output situation.

In eGovernment organizations process mostly follows the exact rules, i.e. they are already pre-defined, so that it often lacks flexibility and speed of the process execution. Causes for this can be endangered treatment of different process-referred tasks. This situation knows bureaucratic completion of existing data or missing support of exceptional cases due to e.g. absence of the partner, by the existing information system, as well as incorrect or

missing allocation access rights of the responsible persons coworkers to necessary documents for the treatment of tasks.

1.2 Administrative processes in eGovernment

Processes in the eGovernment surrounding field, which support functions of the administration, are called administrative processes. The administrative coworkers (internal user) are to guarantee safe handling sensitive data and the use only for process purposes. During the information transfer in administrative organizations one can define two important aspects: on the one hand certain coworkers of the organization of the administration may work on only certain data of customer (external user), on the other hand some administrative processes are lokations spreading; thus the information flow concerns different fields, which are cared for by coworkers from different departments.

The conversion of administrative processes to eGovernment structures requires detail knowledge of the very different kinds of administrative operational sequence in such organizations eGovernment business process therefore exhibits - just like within other ranges like the free economy or the science - different complexity degrees.

The process modelling in the public organizations differs however from that one in enterprises particularly by legal aspects, if as by legal defaults no flexibility is possible and process modelling as well as Process Reengineering close borders are put. Therefore one speaks with the administration of a static sequence organisation contrary to the flexible process cycles with business enterprises. In addition comes still the hierarchical structuring of the public administration, which makes a fast adjustment more difficult to new conditions.

Thus now the organizations and ranges can be identified, within which is eGovernment possible. On the basis of the national administration interfaces result to the citizens (G2C), to here the second sector so mentioned, the economy, and not least to here the third sector so mentioned (von Lucke and Reinermann, 2000). This covers beside non-commercial and non-government organizations used ranges such as universities and hospitals.

1.3 Characteristic of eGovernment process

The eGovernment processes exhibit a set of characteristic characteristics, which differentiate them from other processes. These characteristics must be supported by a IT system:

- Each process is defined, implemented and controlled by an organization. This meant, an institution has such a process

- Special sensitivity because of the execution of sovereign document for natural or legal entities
- High safety requirements with pronounced data security (authentifizierte and encrypted data communication; clear defined access rights; examination and keeping of the user data)
- Constantly available service for the users (24/7)

Thus the next necessary step is the definition of the kinds of role, which are included into eGovernment -processes; these are the external users, i.e. those persons, who take eGovernment processes up and beneficiaries of their results are, as well as internal users, thus the woman employees and coworkers of those institutions, which implement these processes. An external user is a person, who takes a service up, which is implemented by means of a eGovernment process. In the predominant majority of all cases this person does not belong to the implementing organization, however also coworkers of the organizations can request these achievements. This clash of interest is solved by a dynamic division of tasks in the BPS System on architectural level. (Podgayetskaya et al., 2003; Podgayetskaya and Stucky, 2004).

1.4 Solution

In this article is introduced a hybrid process-orientated role and task security model in an Workflow environment (HyPR&A), suitably for eGovernment organizations. The HyPR&A model is based on the RBAC model (NIST, 2002, Sandhu et al., 1996) as well as the model of task and role (Schier, 1999) the characteristic consists of the fact that in this model a relationship from roles, objects and tasks to processes, which are supported by theBPS System is embedded. The HyPR&A concept is based on the consideration that one can control the information flows within a system by the allocation of the roles to tasks as well as the categorization of the roles and objects.

2. SECURITY IN INFORMATION SYSTEMS

With respect to view to IT security with respect to information systems one can differentiate two aspects in the last years for the support from business process cycles with respect to systems: the development of roll-based access control models (RBAC), which are very well for the organization administrative structures in the enterprise and authorities suitable (Eckert, 2003), and process-oriented security models, which are

specific for the business process completion in Workflow systems (Weiner et al., 2003; Hung and Karlapalem, 2003; Botha, 2001).

2.1 Access control in information systems

Access control system can be based on three principles, on DAC (discretionary access control), MAC (mandatory access control) and RBAC (role based access control).

The most important concept from DAC is that the user, who possesses the data is able, the entrance to these data to control. DAC steers the entrance to information based on the identity of the user as well as rules, who specify, which user entrance to which parts of information has DAC functioned only for the controlling of system-oriented resources such as data bases (Pernul, 1992), file systems etc. DAC cannot steer, when access rights can be given or extracted to subjects to objects.

MAC be based on hierarchical security level and assigns its own security stage to each user and each information part or each application. With MAC it can will prevent that a program (in form of a Trojan horse) releases a user file, however cannot not be prevented that a user releases independently his files. With RBAC access rights are bound not directly to a user, but at roles. Roles serve as template for the description of fields. Access rights are assigned to users indirectly by their role affiliation. It is differentiated according to four reference models for RBAC (Sandhu et al., 1996; NIST, 2002): basic RBAC; hierarchical RBAC; constrained RBAC; symmetric RBAC. RBAC supports several well-known security principles: information hiding, leases privilege, separation from tasks as well as data abstraction. However RBAC cannot be used directly to model in order to force security policy, since it was not developed, in order purpose and tasks from data to. (Fischer-Hübner, 2001; He, 2003).

2.2 Security models for Workflow environment

In the past ten years several security models for Workflow environments were developed, among them WAM (Workflow Authoriziation Model), which however only a static beginning for the treatment of the authorization river in the Workflow and data layer support, (Atluri and Huang, 1996) and MLS (Multilevel Security Workflow), which does not know a clear separation between fundamental workflow system components (Atluri et al. 1997).

With the help of roll and were based security model (R&A model) and the CoSAWoE model can the fundamental security requirements be fulfilled

as far as possible, however the administration of resources and communication partners is not regarded here (Schier 1999).

W-RBAC (Weiner et al., 2003) the model contains controlled overwriting of restrictions and places a pair of roll-based entrance control models well-known for workflow systems forwards, generally as W-RBAC-models. In this work it is permitted, a clean separation of the tasks between authorization and workflow aspects of the system for the definition from preferences in the selection of the users, who implement tasks to accomplish.

The Secure Workflow Model of Hung and Karlapalem (2003) concerns itself with problems in heterogeneous environment, in which business processes run, and associated security requirements. In this work an authorizing model with invariants for Workflow in view to agents, events and data is presented and proven that the Workflow execution is safe. Unfortunately this model can be supported only heavily by existing techniques and systems.

The work of Weiner, Bartelmess and Kumar looks similar with their idea. The difference consists of it that by Weiner et al.(2003) as reason for authorizing the RBAC model of Sandhu is used, the control of workflow happens already on access control level. The difference between data flow and supervisory data flow as well as the level of workflow is by Weiner et al. (2003) in the model level missing, the control of workflow effected however because of the use of RBAC.

2.3 Architecture for eGovernment with security requirements

In principle all security models for workflow systems, regarded so far, refer to cross-organizational workflow. The use of RBAC techniques found increasing application within the eGovernment-range (Dridie et al., 2003). In the context of the project Webocracy service architecture CSAP was developed, in which a RBAC system was developed and implemented based on the core RBAC model. In CSAP the administrative requirements for the administration of roles, users and authorizations are implemented (Dridie, 2004). The use of RBAC models in information systems leads to the natural development of security models for workflow systems. Rutgers University's digitally Government Project develops at present in 'Model for dezentralized Workflow change management' (Atluri and Chun, 2003). Software producer Fabasoft offers the product to eGov Suite, the one roll-based organizational model with ACL (access control list) used, the structured and unstructured Workflows for eGovernment supported.

By Podgayetskaya and Stucky (2004) was suggested an IT architecture for eGovernment organizations. This architecture is based on the

consideration, the existing technologies such as Workflow systems or Business Process Support (BPS) systems to use data base systems and web services for typical processes in organizations of the administration. The hierarchical structure of the public administrations is illustrated in the Workflow Enactment service of this model by components, so that the basic requirement of this service is fulfilled: To increase security of the data communication in open systems (Podgayetskaya et al., 2003) One of the most important aspects in this architecture is to cover security. Authentifizierung takes place via a central Registration server. Kerberos protocol are used for thies.

3. HYPR&A – HYBRID PROCESS-ORIENTATED SECURITY MODEL OF ROLE AND TASK

HyPR&A (hybrid process orientated security model of role and task) is a model for organizations of the administration, which support eGovernment - processes, those on the RBAC model (Sandhu et al., 1996; Fischer-Hübner, 2001) as well as are based to the model of task of role (Schier, 1999). In this model a relationship from objects and tasks to processes, which are supported by the BPS System, is embedded. The HyPR&A concept is based on the consideration that one can control the information flows within a system by the allocation of the roles to tasks as well as the categorization of the roles and objects.

3.1 HyPR&A Description

A basic idea of the HyPR&A Sicherheitsmodells lies in the allocation from roles and tasks to processes. The fundamental elements of HyPR&A are processes (P), tasks (A), roles (R), access rights (Z) as well as subjects (s) and objects (O). These elements stand in certain relations to each other.

A subject is called active element of a system. Such an element kannn a change in status cause. The subjects form the subject set of S. An object is called passive element of a system. An object can contain also personal data, e.g. of patient data or student data. The objects do not form the object set of O an element at the same time can actively and passive be.

Resources in the BPS System are all subjects and objects. Resources form a resources set of Ress, which consist of all subjects and objects.

Each system supports certain processes. Each process consists of a set of tasks, which are subject according to the possible processing sequences a partial order.

If the same tasks during different processes or during a process occur several times, they are regarded as different tasks. One can reach this if necessary by name additive and is thus no restriction of the public.

Certain objects are assigned to each process. An object can several processes be assigned at the same time and/or can in different tasks be at the same time worked on. The subjects (e.g. a person or a program), which similar knowledge and abilities have, form certain groups. These groups are called roles.

Roles are partitioned according to the activities by subjects, which fill out these roles, hierarchically. In this kind a role hierarchy is formed. In the information system. In our case we regard suggested architecture for BPS System (Podgayetskaya and Stucky, 2004).

Roles are all subjects, which are grouped after certain abilities for the treatment of the tasks, i.e. certain roles have certain rights to objects. Roles and access rights form in each case the role role of R and the access rights set of Z.

A subject is authorized by the BPS System to exercise certain roles or process tasks. The roles and tasks, which can be filled out and/or settled by subjects, are called authorized roles and authorized tasks.

The roles and tasks, which are filled out in each case and/or settled by subjects at this time, are called actuell roles and actuell tasks.

All data and/or objects during administrative processes, with which during these processes one works, can be differentiated according to five categories (internal_confidential, internal_open, internal_private, external_ private, external_open).

Into the HyPR&A concerning role administration in the BPS System in four categories are divided. Within a category the roll-hierarchical structure is maintained. These categories correspond to structures in organizations of the administration (administrator, process_owner, process_manager, external_user).

The allocation of the categories of objects and roles is represented in table.

Table 1. Interaction of object and role categories

Categorie of objects and roles	internal_confidential	internal_open	internal_private	external_private	external_open
administrator	x	x		x	x
process_owner	x	x	x	x	x
process_manager		x			x
external_user				x	x

Here x means entrance from (categorie of) roles to objects (of objects).

3.2 HyPR&A in Entity Relationship notation

The subjects, objects, tasks, process, roles already and access rights are introduced form in each case the subject set of S, object set of O, task set of A, process set of P, role role of R and access right set of Z. These sets are represented as entity types S, O, A, P, R and Z for the he modelling.

The connections between these entity types are now following-measured as relations represent (whereby some characteristics lead to possible statements across the cardinality (1:n and n:m)).

The relations AP (allocation from tasks to processes) exists, RH (role hierarchy is represented as relationship between arbitrary roles), SR (a relationship between subjects and roles), AR (the role task-dependentness), SA (all possible authorized tasks for subject), SAR (role dependence of task of subject), ZR (relationship from access rights to roles), and OP (relationship from objects to processes).

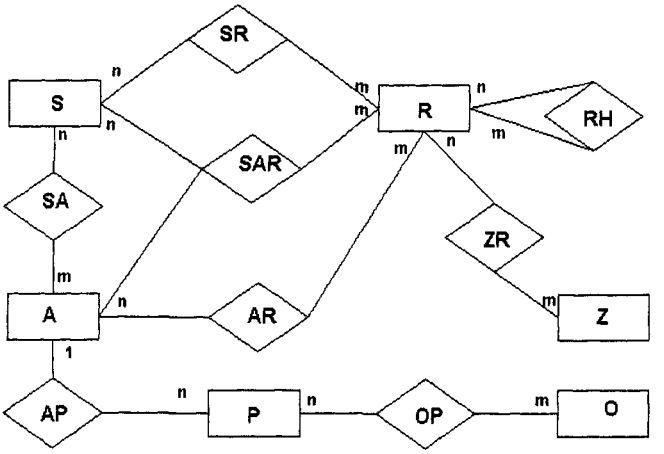

Figure 1. HyPR&A in ERM notation

3.3 Security characteristics

The security characteristics of the model was developed as being certain rules for the security model. These should remain unchanged, so that the model ensures its robustness.

1. Validation

   The relations in HyPR&A support only permitted respectively valid pairs. If the arising pairs in one do not seem to the relationship described

above, they are rejected immediately by the security modeland the further execution of the process is broken off.

2. Object categorization and allocation.
   The objects are first categorized and assigned afterwards to processes.

3. Role categorization and allocation.
   The categorization of the roles applies to each role. Within a category incomparable pairs can be. It is to be stressed that this rule does not stand in the contradiction for hereditary relationship with the right assignment, because this follows the roll-hierarchical principle.

Table 2. Example

category	hierachy	role	subject
external_user	1	graduate students	Mr. Studentmann
	0	undergraduate students	
	1	tutor	

Possible roll-hierarchical structures within this category
{graduate students(subject), undergraduate students(subject)}, so that undergraduate students(subject) < graduate students(subject) – {0 < 1} ;
{tutor(subject), undergraduate students(subject), so that undergraduate students(subject) < tutor(subject) – {0 < 1}.
Determined pairs, e.g. {tutor(subject), graduate student(subject)} one can regard as incomparable pairs for subject.

4. Task-Role-Subject
   A subject can select several tasks as well as several roles within a process, if these tasks for it are authorized (definition, relation SA) and if the subject is assigned to an authorized role (definition, relation SR). A subject may update these tasks (to settle), if it is justified due to the task(s)-role(s) relationship to it (relation SAR).

5. Subject Object Relationship
   A subject can access the objects within the process, if the authorized role as well as the tasks (relations SA, SR) are categorized valid and the role(s).
   A subject may access several objects within the process, if a combination of role(s) – task(s) pair(s) valid for it, exists (relation SAR) and the allocation object role category is correct (table 1). This means that certain conditions must be fulfilled. A subject may accept several roles, which are not mutually exclusive. Further the subject in this role or one of these roles must be allowed to settle the assigned tasks.

Finally it must be examined whether the intended role(s) – task(s) combination is valid. Only if these conditions are fulfilled, the possibility that this subject in these roles may access this object exists, in order to settle the tasks within this process.

3.4 HyPR&A model as RBAC and Workflow Unit

We plot HyPR&A. Here (Figure 2) the two ranges workflow unit and role-based beginning are shown as RBAC for the conversion in an information or a BPS system. The connection between Rbac and Workflow architecture consists of the roles and objects, which the information or BPS system contains.

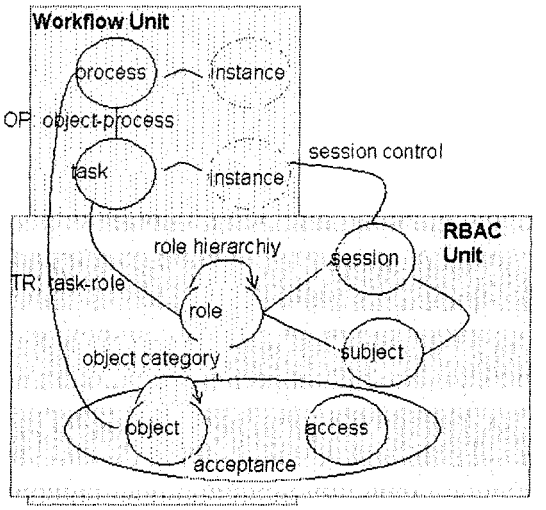

Figure 2. HyPR&A as workflow and RBAC units

The structure of HyPR&A is adapted to the architecture of the Workflow Enactment service and/or to the architecture of the Workflow engines (Podgayetskaya and Stucky, 2004). The HyPR&A structure is two-dimensional: the vertical level consists the Workflow unit, horizontal has the RBAC unit. The Workflow represents the control and data flow, thus on the one hand the respective tasks and their processes as well as on the other hand in and to outgoing data each the tasks. In HyPR&A the supervisory data flow marks the allocation from objects to processes as well as from tasks to processes. Data flow clarifies the allocation of roles and objects as well as of tasks and roles.

3.5 HyPR&A during the registration process

The expiration of registration is a ordinary process in numerous organizations of the administration such as hospitals (patient admission), citizen office or universities (seminar -, examination registration). This process is identified-drawn due to the active participation of external users as external process. For the expiration of registration the following steps are characteristic:

1. The user selects exactly one process, which he/she needs with the announcing procedure[1]
2. Afterwards he/they registers the necessary data e.g. in the form and
3. sends or hands this to the registration office over for further treatment

Here a process in a university one regards. We represent only registration for an examination. A subject is assoziert in this case with a studying. The role designated student for this role category (external user). In Figure 3 (left) is sketched this external announcing process in Petri Net notation. Figure 3 (right) points the HyPR&A support of this announcing process, thus the assignment of objects to roles and tasks as well as the expiration of assignment of appropriate access rights to a subject.

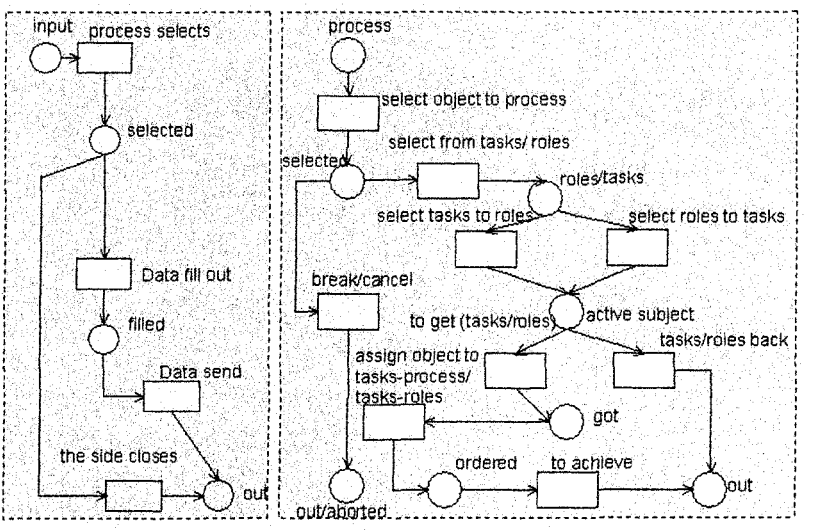

Figure 3. Cutout from external processes: on the left of expiration of announcing, on the access rights assignment in HyPR&A

[1] Within a process one can differentiate several process procedures, e.g. as registration with respect to the citizen office can only registration to the examination with respect to a university.

In the first step of the announcing procedure the objects are assigned to processes. But the necessary pairs from the relationship OP (object-process) are selected by the BPS system. According to the rules 2 and 3 is already categorized the roles as well as the assigned objects.

If the external user breaks the announcing procedure off and/or closes the side, the support of the process is broken off in accordance with HyPR&A by the BPS system. Also in the case the fact that the role selected task and/or the task of the roles enspricht (corresponds), e.g. the task may not do only by external user is implemented, the arrangement to objects refused and further not accomplished (Figure right; rule 1).

If an external user wants to resume the announcing procedure, certain tasks are assigned to the process (relationship task-process AP) and thus makes possible for the subject to exercise it.

HyPR&A ensures for the fact that these tasks of roles are assigned, which settle this role (can) to be able or that turned around this role for this assigned task during the process for the practice of the tasks responsibly is (relationship of task-roles AR).

The subject will update the role and/or tasks (relationship SA, SR) and only for it permitted role tasks - combinations during this process exercise (SAR relationship, rule 4). This corresponds to step 2 of the announcing procedure 'filling out the form'.

For execution of the third step 'delivery of the form to the registration office' rule 5(subject object relationship) is used over the assigned rights for the subject (relationship RZ). This means: the subject updates the role and tasks and has the possibility of exercising this role and of implementing the tasks. The data of the subject in an object of the category are external_private stored and passed on from the system to the treatment.

So only one role can be assigned as external users and only with the ensprechenden tasks, which are intended for this process and this role, during this process. The objects are assigned to the process in the system, so that according to categorization the respective process one makes.

The external as well as internal processes can contain confidential data. These data will be categorized in our model as well as in the system as internal_confidential, internal_private or external_private objects. The available case concerns only external_private objects.

For the treatment of the process in rule or several staff member of the organization is responsible. Therefore it is meaningful to assign to tasks of working on certain roles. Certain roles are responsible for certain tasks, therefore the sequence of the role tasks is not relevant - or task role arrangement.

The following allocation is made by the BPS system (table 3):

Table 3. HyPR&A allocation by BPS system

process	registration
category of object	external_private
object	person_date
category of role	external_user
role	student
	fill data
task	send data
	close site
subject	M. Mustermann

The execution of HyPR&A is independent of the process procedure, i.e. the HyPR&A rules apply to all processes, which are supported by the information and/or BPS system. Reason for it is the choice of the process as the first step, afterwards follows the independent allocation of tasks, roles and objects, which belong to this process.

4. SUMMARY

In this article a security model HyPR&A is suggested, which can be adapted to safety requirements in organizations of the administration. HyPR&A combines the conception of roles and objects in both concepts: Workflow and RBAC. This has the consequence that in accordance with the allocation to roles and tasks as well as from objects to processes access rights are assigned to the subjects

The structure of HyPR&A is adapted to the architecture of the Workflow Enactment service and/or to the architecture of the Workflow engines. The supervisory data flow runs in both directions: vertically and horizontal. Roles and objects are connected with the expiration component, which represents the processes in the information or BPS system.

A impotant aspect in the interaction of the architecture BPS system and the security model is the analysis and modelling of the Workflow models for applications. The safety requirements in the Workflow models presented here concern the data security. Due to its structure consisting of two units HyPR&A is well suitable for the support of these requirements. The structure of the Workflow unit corresponds to the expirations, objects and roles of the Workflow models; the RBAC unit exercises according to access supervision the roles. For the implementation of HyPR&A these Workflow models are thus in ancestor leaning to the suggested architecture BPS system respectively the Workflow engine developed.

At present exists no universal safety model, which fits for each system ideally and can cover all security requirements 100%. Therefore its own security model should be developed just like the processes themselves running in the system for each system on the basis of existing classical

security models. HyPR&A, hybrid process-oriented security model of role and tasks, functioned in Workflow environments and is geeiget only for organizations of the administration, whose tasks, roles and data are connected with processes and their process cycles are more or less vordefinert. For this reason accurate categorization comes of objects and roles.

5. REFERENCES

Atluri, V. and Chun, S.A., 2003, Handling Dynamic Changes in Decentralized Workflow Execution Environments, *DEXA 2003 Proceedings*: P. 813 - 825.

Atluri, V. and Huang W.-K. , 1996, An Authorization Model for Workflows, Proceedings of the 4th European Symposium on Research in Computer Security: *Computer Security*: P. 44 – 64.

Atluri, V., Huang W.-K. and Bertino, E., 1997, An Execution Model for Multilevel Seccure Workflows, *Proceedings of the IFIP TC11 WG11.3*: P. 151 – 165.

Botha, R.A.., 2001, CoSAWoE - A Model for Context-sensitive Access Control in Workflow Environments. *Dissertation, Rand Afrikaans University* i.Br.

Dridi, F., Muschall, B., Pernul, G., 2003, An Administration Console for the CSAP System. In: *Short Paper Proceedings of the 15th Conference on Advanced Information Systems Engineering (CAiSE 2003):* P.345-350.

Dridi, F., Muschall, B.and Pernul, G., 2004., Administration of an RBAC System. Proc.of the 37th Hawaiian International Conference on System Sciences (HICSS 2004):P. 1014-1026

Eckert, C., 2003, IT-Sicherheit. Oldenburg.

Fischer-Hübner, S., 2001, IT-Security and Privacy: Springer Berlin et al.

He,Q., 2003, Privacy Enforcement with an Extended Role-Based Access Control Model NCSU *Computer Science Technical Report TR-2003-09.*

Hung, P. C. K., Karlapalem K.: A secure workflow. Proceedings of the Australasian information security workshop conference on ACSW, 2003, V21: P. 33 – 41.

Pernul, G.,1992, Security Constraint Processing During Multilevel Secure Database Design, in *Proceedings of Eighth Annual IEEE Computer Security Applications Conference,*: P. 229-247.

NIST, 2002, The Economic Impact of Role Based Access Control. Research Triangle Institute. *NIST Planning Report 02-01*..

Podgayetskaya, T., Ratz, D. and Stucky, W., 2003, Modell eines Workflow-Systems zur Erhöhung der Sicherheit von Web Services, Proceedings E. Otner (Hrsg.) in Symposium Entwicklung Web-Services basierter Anwendungen. In Rahmen der 33. Jahrestagung der GI: P. 37-52.

Podgayetskaya, T., Stucky, W., 2004, A Model of Business Process Support System for E-Government. DEXA 2004 *Proceedings. Published by the IEEE Computer Society,* P2195: P.1007-1015.

Sandhu, R.S., Coyne, E. J., Feinstein, H.L. and Youman, C.E., 1996, Role-Based Access Control Models, *IEEE Computer* 29(2): P. 38- 47.

Sandhu, R.S., Ferraiolo, D. F., Kuhn, D. R., 200, The NIST Model for Role Based Access Control: Towards a Unified Standard, Proceedings, 5th ACM Workshop on Role Based Access Control, P.26-37.

Schier, K., 1999, Vertraurenswürdige Kommunikation im elektronischen Zahlungsverkehr. *Dissertation*, Universität Hamburg i.Br.

Wainer, J., Barthelmess, P., and Kumar, A, 2003, W-RBAC - A Workflow Security Model *Incorporating Controlled Overriding of Constraints. J of Coop. Inf. Sys.4*,: P. 455-48.