# BusiROLE: A Model for Integrating Business Roles into Identity Management

Ludwig Fuchs[1], Anton Preis[2]

[1] Department of Information Systems,
University of Regensburg, 93053 Regensburg, Germany
Ludwig.Fuchs@wiwi.uni-regensburg.de
[2] Institute of Management Accounting and Control
WHU – Otto Beisheim School of Management, Burgplatz 2, 56179 Vallendar, Germany
Anton.Preis@whu.edu

**Abstract.** The complexity of modern organisations' IT landscapes has grown dramatically over the last decades. Many enterprises initiate role projects in order to reorganise their access structures based on an organisation-wide Identity Management Infrastructure (IdMI). This paper surveys role models and related literature and identifies different role properties. It shows that current role models are not feasible for their usage in IdMIs. By implementing one single type of role they fail to take business requirements and different role perceptions into account. This paper improves the current situation by developing busiROLE, a role model that integrates various types of roles, fulfilling business- as well as IT requirements, and is hence usable in IdMIs.

**Keywords:** Identity Management, Business Roles, Compliance, IT security.

## 1 Introduction and Motivation

Large companies have to manage complex organisational structures and a large number of identities within their IT systems. As a result of incorrect account management users accumulate a number of excessive rights over time, violating the principle of the least privilege [1]. This situation results in a so called identity chaos. Implementation projects like [2] and studies [3] show that major security problems arise because of employees gaining unauthorized access to resources. National and international regulations like Basel II [4], the Sarbanes-Oxley Act [5], and the EU Directive 95/46 [6] together with internal guidelines and policies force enterprises to audit the actions within their systems. Roles are seen as means to meet compliance demands in general. Yet, implementing a technical IdMI as presented in [7] is only the starting point for getting compliant. IdM is not able to take business needs into consideration on a purely technical level. Organisational IdM integrates business requirements into global user management processes. Its understanding of roles is shifted from a rights-based towards a task- and organisation-oriented role concept [8]. Nevertheless, companies and IdM vendors mainly implement a basic role model [9] which defines one single type of role only. The main problem is that various types of roles, e.g. Business Roles, Organisational Roles, Basic Roles, or IT Roles exist within the company without any model that defines and standardises the relations between them. However, as IdM has the goal to essentially connect the technical IT layer with

the business perspective, it needs to be able to integrate these different kinds of roles. Bertino et al. [10] likewise mention that Enterprise Security Management tools like IdM solutions don't conform to basic Role-Based Access Control (RBAC) even though they are generally considered to be among the most important RBAC applications. The goal of this paper is to improve that situation by introducing busiROLE, a role model which integrates the different types of roles needed in IdMIs. BusiROLE is also currently used as the underlying formal model during the process of role development and the whole lifecycle of a role system as presented in [11].
This paper is structured as follows. In section 2, related work is presented. A survey of existing role models and properties in section 3 gives an overview and a classification of well-known properties of classic role models. Section 4 subsequently introduces busiROLE explaining the different components, showing their peculiarities and relationships. Finally, conclusions and future work are given in section 5.

## 2 Related Work

### 2.1 In-house Identity Management

Over the last few years in-house IdM, i.e. Identity Management within the IT infrastructure of companies, has established itself as a core component of Enterprise Security Management. It deals with the storage, administration, and usage of digital identities during their lifecycle. The aforementioned identity chaos needs to be faced by implementing a centralised IdMI as shown in [7]. Its main building blocks are a Directory Service, User Management, Access Management, and an Auditing Module. Directory Services provide synchronised identity information that is facilitated by the other components. User Management e.g. deals with the provisioning of users, granting and revoking access to resources. When users logon to certain applications, Access Management controls the access to the requested resource while users' as well as administrators' activities are logged within the Auditing Module. IdM duties cover rather simple tasks like automatic allocation and revocation of user resources. However, they also include sophisticated tasks like role management.

### 2.2 RBAC and Role Types

Role-Based Access Control is a widely used access control paradigm. In its original sense users are assigned to roles and roles are associated with permissions that determine what operations a user can perform on information objects acting as a role member. Besides a more secure and efficient user- and resource management, manual administration efforts are minimised and compliance issues addressed by the usage of roles [12]. Numerous role models have evolved as a result of special industry needs. Additionally, the difference between IT- and business- related roles has been discussed intensively [1]. Roles on the IT layer are essentially bundles of permissions within an application. Business related roles are defined on work patterns, tasks, and the position of employees within the organisation. Both concepts can be connected by defining the permissions that are needed to perform the various tasks. Table 1 gives a short overview over their main characteristics according to their application level.

**Table 1.** Role characteristics according to application layer.

| *Criterion* | *Business layer* | *IT layer* |
|---|---|---|
| Role concept | Organisation-, task-, competence-oriented | Rights-based |
| Application area | Business processes, workflows, task bundles | Local application, IT system |
| Responsibilities | Business manager, process owner | IT administrator |

Adjacent research areas, e.g. company-wide authorisation models and role engineering approaches work with a business-related perception. The Stanford Model [13] for instance integrates *tasks* and *functions* of employees in its architecture. Even though this model attempts to manage the relationships between components in a structured way, its complexity makes the adoption in an IdMI hardly manageable. Wortmann [14] introduces the concept of *person*, *process-role*, and *tasks* in his approach. Still, coming from a process-oriented background, he focuses on the operational structuring and omits organisational structures. Yet, this integration is of major importance for organisational IdM. Some role engineering approaches like [15] or [16] also work with a business-related definition of the term *role*. Epstein [15] introduces entities like *job* or *workpattern* but does not relate them to business needs.

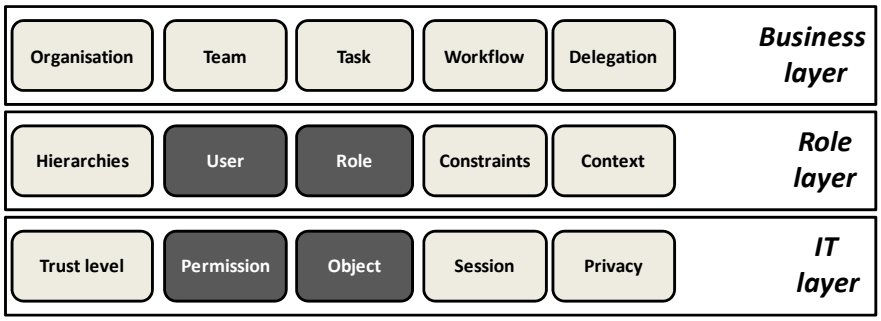


**Fig. 1.** Role properties and their classification. The IT layer represents the system resources. The Role layer acts as intermediary between IT- and organisational aspects. Role layer properties can be closer to business or IT aspects or even appear on all layers. The Business layer represent both the static (organisational structure) and dynamic aspects (operational structure) of organisations and their interdependencies known from organisational theory [17].

## 3 Role Properties – Overview, Classification, and Survey

In order to define a generic role model in terms of organisational IdM we start by analysing role properties. Each role model implements a subset of those properties, interpreting the term *role* in its own notion. We use a classification splitting the organisation into a Business-, a Role-, and an IT layer (Fig. 1). Note that properties are classified according to their usage in the according role models. Privacy or Trust, e.g., can be regarded as business- related but are used in a technical manner in the surveyed models. Hence they are located at the IT layer. In general this framework firstly relates role properties to the corresponding layer and secondly differentiates between core- and extensional properties. This way we are able show whether a role

model is rather resource- or business- oriented. Analysing 17 major role models we were able to identify 15 different role properties. *Role*, *User*, *Permission*, and *Object* are the core components of every surveyed model. Additional properties surround these central components leading to a functional extension of a role model. Hence they are classified as extensional properties. In the following we are going to shortly present the properties known from the RBAC literature in tables 2 – 4.

**Table 2.** IT layer Properties.

| Property | Description |
|---|---|
| Object (OBJ) | Represents a system resource. The collectivity of all objects represents the set of all resources of an IT system operations can be performed on. |
| Permission (PRMS) | Represents the right to perform an operation on an OBJ. We represent a permission as a pair *(am, o)* where *am* is an access mode, identifying a particular operation that can be performed on the object *o*. |
| Session (SESSION) | Sessions are necessary to enable and document user and role activities. Once a role is activated, a session has to be started. |
| Trust levels (TRUST) | Trust levels help to differentiate between security levels. Objects as well as roles can have different trust levels. Trust levels of objects must be determined whereas role trust levels can e.g. be earned by trustworthy behaviour. Trust levels can be modelled as attributes, for instance. |
| Privacy (PRIV) | Privacy refers to the security of personal data. Models with a privacy property refer to the protection of personal related data. Similar to TRUST, modelling of PRIV can be done using attributes. |

**Table 3.** Role layer Properties.

| Property | Description |
|---|---|
| Role (ROLE) | From an IT-related point of view, a role can be a bundle of permissions to operate on certain IT- or systemic objects. From an organisational perspective, however, a role is a link from an organisational property to an employee who for example has to fulfill a certain task within a team or a context. |
| User (USER) | A person who is assigned to a certain role. From a more systemic point of view a user needn't necessarily be human and can even be part of an IT process that is assigned to a role. |
| Hierarchies (HIER) | Among roles, there can be hierarchical relations. Permissions can be inherited from one role by another. Additionally work can be delegated using a role hierarchy. |
| Constraints (CONSTR) | Refer to the relations among different role properties. They can appear in every layer. With them, limitations and rules are formed. Other properties, e.g. contexts, can be modeled by constraints. |
| Context (CTXT) | Represents the circumstances in which roles are activated. An example could be an emergency case where the activation of a number of special roles with clearly defined permissions is necessary. |

**Table 4.** Business layer Properties.

| Property | Description |
|---|---|
| Organisation (ORG) | An organisation can be divided into organisational- and operational structure. The latter includes dynamic aspects like TASK, WFL, and partially even TEAM structures. Organisational structures represent the different hierarchy types and their entities within the organisation. |
| Task (TASK) | Represents a certain job or duty that has to be fulfilled with regards to a specified outcome. A task can consist of several partial tasks or subtasks. Tasks also can be pooled and then form task groups. |
| Workflow (WFL) | A subtask consists of workflow units. Ultimately, a workflow has to result in a certain outcome, which makes it similar to tasks. Unlike tasks, the focus lies on the sequence of steps to be performed. |
| Team (TEAM) | A very narrow definition of this property could be a user pool. Teams are task- and goal-oriented [18]. The component can be seen as in-between of organisational and operational structures. |
| Delegation (DELEG) | The term *delegation* has a two-sided meaning: First, it can be total when e.g. whole roles are delegated from one user to another Second, the delegation can also be partial and be only valid for single tasks. Delegation is closely connected to the role hierarchies from table 3. |

**Model Survey and Overview**

We are now going to present an abstract of our role model survey. Due to space limitations, we are focusing on the discovered role properties and their usage in existing role models. For the same reason we are additionally not referencing every single model separately in the references section. Many of them can be found in [1]. Throughout the survey, every considered role model has been visualised using the three-layer classification introduced at the beginning of this section. Figure 2 sums up the classification results. The tableau shows for instance that TrustBAC [19] implements *Role Hierarchies*, *Constraints*, *Sessions*, and extends basic RBAC functionality using system-specific *Trust Levels*. Moreover it points out that none of the business properties are realised in TrustBAC. We are aware that this tableau only gives a qualitative impression as there is no standardised definition used among all models for the single role properties. Nevertheless it points out the core properties that are implemented by all role models. One can also see that most role models are IT-oriented. Even though some of them are implementing business properties, e.g. ORBAC [20], none of the models is really business-focused and therefore feasible for role-based IdM deployments. The most powerful model concerning the representation of business properties is the SRBAC model, [21] as it is capable of modelling organisational structure and functional units. It has, however, a limited definition of hierarchies. The central outcome of our analysis is that the models each define only one single type of roles. The basic RBAC family [9], even though it is used in most IdM deployments, can also not meet the requirement of multiple role types. This result complies with and underlines Bertino et al.'s finding [10] that the RBAC family is not feasible for usage in Enterprise Security Management Infrastructures.

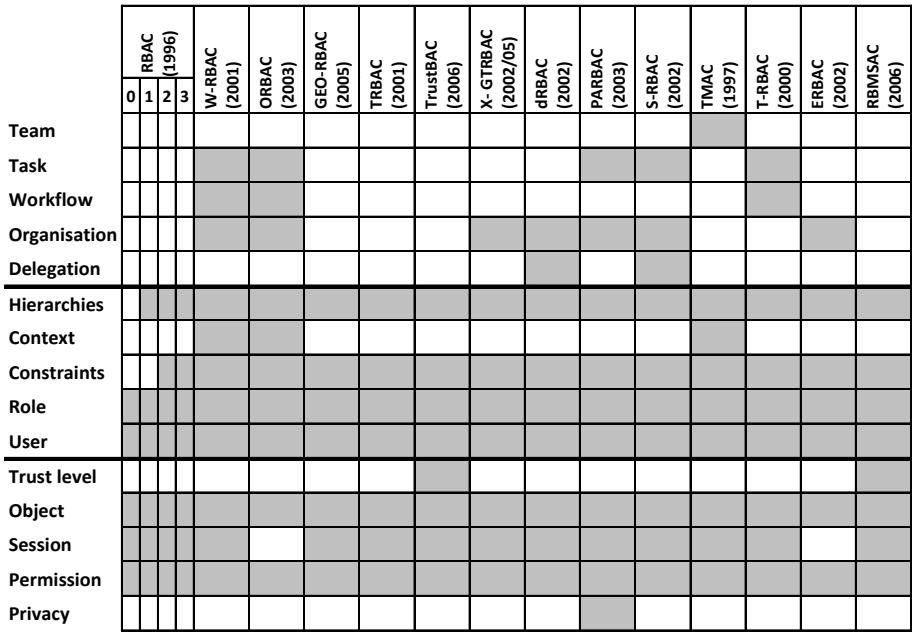


**Fig. 2.** Survey of existing role models. The first vertical column lists the role properties while the horizontal axis represents the various role models. Grey colouring indicates that an according property is realised in a certain role model. Unavailable functionalities remain white.

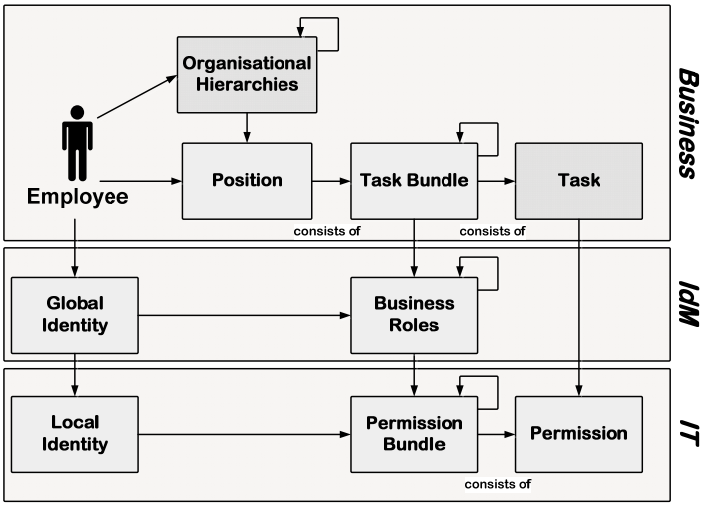


**Fig. 3.** BusiROLE. The business properties form the organisational basis. Their relationships represent the hierarchical dependencies and an increasing granularity level, from Organisational Hierarchies and Positions towards Task Bundles and singular Tasks.

## 4 BusiROLE – Integrating Business Role types into IdM

In the following we define the properties and the types of roles needed for successful role deployment in Identity Management solutions. We argue that the integration of more than one role type is necessary to take business structures and requirements into account. In busiROLE every employee has a number of different roles that stem from his position in various Organisational Hierarchies and his assigned Task Bundles. Figure 3 shows the busiROLE core entities and role types derived: On the Business layer we integrate different types of *Organisational Hierarchies* (Basic Roles), *Positions* (Organisational Roles), *Task Bundles* (Functional Roles), and *Tasks*. The *Business Roles* entity is the core component of our model. It represents the collectivity of an employee's roles. Note that we also could have modelled each role type separately and connected it with the corresponding business entity. However, for clarity reasons the Business Roles entity bundles all the different role types seen in figure 4. We furthermore introduce an *Employee* entity and an according *Global Identity* that links to all application-specific user accounts (*Local Identity*). On the IT layer we use *Permission Bundles* which can be expressed e.g. using local IT Roles. This feature is needed to connect local systems with different permission handling mechanisms to a global IdMI. However, we are not going into detail about the IT layer elements as we adopt the well-known resource-oriented RBAC-approach [9] on this layer.

### 4.1 Business Layer Properties

According to organisational theory a firm's global goal is split up into sub-goals and assigned to single organisational units (see figure 4). Employees' responsibilities are defined by what they do, who they report to, and who reports to them. These

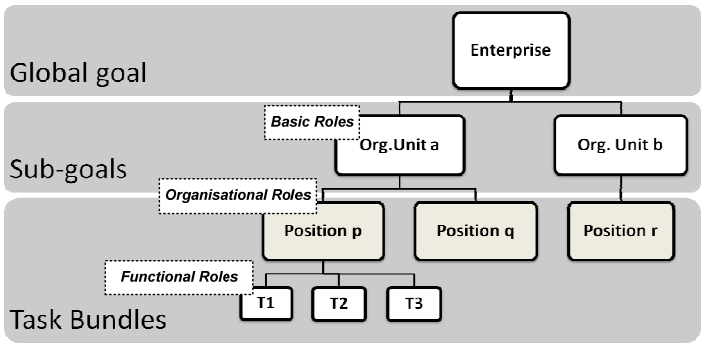


**Fig. 4.** Organisational goal, Sub-goals, and Task Bundles. As long as a goal is too complex for the assignment to an employee we speak of goals and sub-goals. Sub-goals are split into Task Bundles that are assigned to certain positions.

definitions are assigned to positions rather than to specific individuals. The positions are in turn assigned to predefined work packages. Scientific publications in the business administration area and in the area of organisational behaviour contain a profound theoretical insight into relevant facts and relations within an organisation [17], [22]. Our survey in section 3 has shown that up to now no suitable role model for IdMIs exists, mostly because of missing a differentiation between role types and hence business layer properties. We argue that organisational structure, rather than operational structure, is the main pillar of a role model in IdMIs. Operational structures, i.e. process-, workflow-, and single task definitions are not feasible within IdMIs. On the one hand it is not possible to keep a complete process- and workflow database up-to-date within an organisation. On the other hand existing IdMIs already are closely related to the line organisation making it easily extensible.

**Employee:**
BusiROLE needs to be capable of assigning existing Positions and Task Bundles to the according persons based on different hierarchy types within the enterprise. We hence extend and split the *User* concept known from the original classification in figure 1: The business property *Employee* is introduced as the counterpart of a *Global Identity* representing the core user account within the IdMI on the Role layer. *Local Identities* are the user accounts of employees on the IT layer. This structuring is already well known from the implementation in most IdM solutions.

**Organisational Hierarchies (Basic Roles):**
As mentioned beforehand, IdM solutions are already closely aligned to the organisational structure of an enterprise. Organisational Hierarchies can be used to represent the Basic Roles of employees, i.e. permissions that every employee in a certain organisational unit is granted. The *Organisation* property from our original classification, however, has to be extended in order to be able to represent any kind of hierarchical structure. Besides the line organisation IdM solutions have to be able to integrate e.g. a financial- or a reporting hierarchy. A team can also be regarded as a (temporary) organisational unit. We hence omit teams as a separate busiROLE entity. Two employees could e.g. have the same position in the line organisation and consecutively the same Functional Roles derived from that position, however, one of them might have a special Task Bundle related to a team where he is member of. This is represented using a different Organisational Hierarchy type which contains existing team structures and related positions as well as Task Bundles.

**Position (Organisational Role):**
Positions are needed to represent functional entities within organisational hierarchy elements. They are regarded as Organisational Roles and abstract descriptions of a collection of Task Bundles assigned to certain employees. An example would be a *Windows Developer* within the *Development* department. SRBAC [21], e.g., is already working with so called functional units which are able to represent IdM requirements regarding job positions. Note that there is a relationship between the Organisational Roles and the Basic Roles.

**Task Bundle (Functional Role) and Task:**
Taking a closer look at the *Task* property from the classification in section 3 one can see that existing definitions are not able to model Task Bundles, i.e. hierarchical structures within *n* available tasks. Task Bundles are essentially the Functional Roles of employees. Task Bundles are defined by business representatives according to the sub-goal of an organisational unit and the qualification and workload of an employee. Note that they are only assigned to a position if their complexity allows treatment by a single employee. If no Task Bundles are defined for a certain Position, the Position itself is representing the complete Task Bundle of an employee (see figure 4). Note that Task Bundles also might not necessarily be connected with a Position but directly related to an Organisational Hierarchy element. For example, a manager might assign a special duty to one employee independent from his position within the organisation. Another conceivable scenario could be delegated Functional Roles.

### 4.2 IdM Layer Properties

After having presented the required business properties we are going to examine the IdM layer properties of busiROLE. Note that the definition of the Role layer from our survey differs to the understanding of our IdM Layer: Many of the role models define the Role layer as the Access Control layer on top of the permissions within an application. In our context, the IdM layer is comprised of the Business Roles and their properties managed within the organisation-wide IdMI. Local IT Roles or permission bundles as they are used in the existing models are a part of the IT layer in our approach.

**Global Identity:**
As mentioned beforehand we introduce a global identifier for each employee. Every single application-specific user account is mapped to exactly one global ID in order to be able to activate and deactivate it automatically via resource provisioning processes of the IdM. This feature is well known from available IdM solutions.

**Business Roles:**
We define the *Business Roles* entity as the IdM representation of an employee's Basic-, Organisational-, and Functional Roles. Business Roles essentially connect the task-oriented business view with the resource-oriented IT layer, integrating the different types of roles needed within an IdMI. Additionally, they are able to include technical measures like Trust or Privacy as we know them from our original classification. For usability and management reasons we argue that the granularity level for a direct connection of Business Roles with Tasks is too high as a single Task does not represent an independent role within the enterprise. Hence Business Roles only represent Task Bundles, Positions, and Organisational Hierarchy elements in

form of the different role types. BusiROLE directly relates Task Bundles and Business Roles, nevertheless if a company has not defined fine grained Functional Roles (i.e. Task Bundles), Positions are essentially representing the Task Bundle of an employee (see figure 4). However, note that such a situation limits the usability and the flexibility of busiROLE: Delegation could only be conducted on position (i.e. Organisational Role) level and additionally the different permutations of Task Bundles assigned to a Position could not be modelled accurately. Redundancy issues within the role definitions would complicate the role management.

### 4.3 Global and Extensional Properties

In the following, we are going to introduce two global properties and four extensional, hence not mandatory properties of busiROLE. They are not modelled as entities but as attributes of core entities.

**Constraints and Context:**
Constraints and context are global properties that influence all entities and their relationships. Using the definition given in section 3, constraints can be viewed as conditions imposed on the relationships, assignments, and entities. An Employee acting in the Organisational Role of a financial manager may not be allowed to act as a financial auditor at the same time (separation of duty). We are expressing them in terms of system-, entity-, or relationship policies. Using a context, we can model certain exceptional circumstances in which a particular role can be activated.

**Workflow, Delegation, Trust, and Privacy:**
Those four properties from figure 1 are handled as extensional properties. Delegation functionality can be implemented as an attribute of a Position. Organisational policy defines which employees can be appointed as representative of another employee under exceptional circumstances. Workflows known from various role models like [23] and [24] are not originally integrated within IdMIs. Within bigger companies it is impossible to maintain a workflow base which represents all existing workflows in combination with the needed permissions at a certain point of time. As aforementioned this is an aspect where our model differs from existing operational-based approaches (like [14]).

## 5 Conclusions and Future Work

This paper has shown that widely used basic RBAC models are not feasible for their usage in modern IdM because each only implements one single type of role. On basis of a short survey we hence presented busiROLE, a role model able to integrate role types needed in organisational IdMIs, namely Basic Roles, Organisational Roles, Functional Roles, and IT Roles. Its biggest advantage compared to existing models is the usability in organisation-wide and application-independent IdMIs. On the basis of busiROLE, modern IdM vendors as well as big enterprises operating an IdMI are able to closely connect business objectives and technical user management. BusiROLE provides the capability to represent business structures within the company-wide IdMI. Hence it fosters the business-oriented development, management, and

maintenance of roles. It is furthermore independent from local Access Control Mechanisms, making it easy to integrate several different target systems. It is currently used as the core model of our hybrid role development approach. Future work includes the introduction of customisable position types in order to provide reusable single position patterns. We furthermore are going to investigate the hierarchical relations among the different role types. Besides such theoretical extensions and improvements busiROLE is going to be tested within different Identity Management Infrastructures. This way the advantages of different role types within one IdMI can be made visible.

**Acknowledgments.** The work reported in this paper will be continued within the SPIKE project which is funded by the European Union under the Seventh Framework Program (Contract No. 217098).

## References

[1] Ferraiolo, D. F., Kuhn, R. D., Chandramouli, R.: Role-Based Access Control. Artech House, Boston, Mass./London (2007).

[2] Larsson, E. A.: A case study: implementing novell identity management at Drew University. In: Proceedings of the 33rd annual ACM SIGUCCS conference on User services, Monterey, CA, USA (2005), http://doi.acm.org/10.1145/1099435.1099472

[3] Dhillon, G.: Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. Computers & Security 20 (2), 165-172 (2001).

[4] Bank for International Settlements BIS: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version (2006), http://www.bis.org/publ/bcbs128.pdf

[5] Sarbanes, P. S., Oxley, M.: Sarbanes-Oxley Act of 2002, also known as the "Public Company Accounting Reform and Investor Protection Act of 2002" (2002), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf

[6] European Union: Directive 95/46/EC of the European Parliament and of the Council. Official Journal of the European Communities L (28-31) (1995), http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[7] Fuchs, L., Pernul, G.: Supporting Compliant and Secure User Handling – a Structured Approach for In-house Identity Management. In: Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES '07), Vienna, Austria (2007), http://dx.doi.org/10.1109/ARES.2007.145

[8] Walther, I., Gilleßen, S., Gebhard, M.: Ein Bezugsrahmen für Rollen in Unternehmungen. Teil 2: Klassifizierung von Rollen und Situationen. Working Paper 1/2004, University of Erlangen-Nürnberg, Department of Wirtschaftsinformatik I (2004), http://www.forsip.de/download.php?file=/publikationen/siprum/iw-sg_arbeitsbericht_2.pdf

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

[10] Li, N., Byun J., Bertino, E.: A Critique of the ANSI Standard on Role-Based Access Control. IEEE Security&Privacy 5 (6) 41-49 (2007).

[11] Fuchs L., Pernul, G.: proROLE: A Process-oriented Lifecycle Model for Role Systems. In: Proceedings of the 16th European Conference on Information Systems (ECIS), Galway, Ireland (2008).

[12] Gallaher, M. P., O'Connor, A. C., Kropp, B.: The economic impact of role-based access control. Planning report 02-1, National Institute of Standards and Technology, Gaithersburg, MD (2002), http://www.nist.gov/director/prog-ofc/report02-1.pdf

[13] McRae, R.: The Stanford Model for Access Control Administration, Stanford University (unpublished) (2002)

[14] Wortmann, F.: Vorgehensmodelle für die rollenbasierte Autorisierung in heterogenen Systemlandschaften. Wirtschaftsinformatik 49(6), 439-447 (2007).

[15] Epstein, P., Sandhu, R.: Engineering of Role/Permission Assignments. In: Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC'01), New Orleans, LA, USA (2001), http://doi.ieeecomputersociety.org/10.1109/ACSAC.2001.991529

[16] Roeckle, H., Schimpf, G., Weidinger, R.: Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization. In: Proceedings of the fifth ACM workshop on Role-based access control, Berlin, Germany, (2000), http://doi.acm.org/10.1145/344287.344308

[17] Mintzberg, H.: Structuring of Organizations. Prentice Hall, Englewood Cliffs, N.J. (1979).

[18] Katzenbach, J. R., Smith, D. K.: The Wisdom of Teams: Creating the High-Performance Organization. Harvard Business School Press, Boston, Mass (1993).

[19] Chakraborty, S., Ray, I.: TrustBAC: integrating trust relationships into the RBAC model for access control in open systems. In: Proceedings of the eleventh ACM symposium on Access control models and technologies, Lake Tahoe, CA, USA, (2006), http://doi.acm.org/10.1145/1133058.1133067

[20] El Kalam, A. A., Benferhat, S., Miege, A., El Baida, R., Cuppens, F., Saurel, C., Balbiani, P., Deswarte, Y., Trouessin, G.: Organization based access control. In: Proceedings of the Fourth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'03), Lake Como, Italy, June 2003, 120-131 (2003), http://doi.ieeecomputersociety.org/10.1109/POLICY.2003.1206966

[21] Seufert, S. E.: Der Entwurf strukturierter rollenbasierter Zugriffskontrollmodelle. Informatik – Forschung und Entwicklung 17(1), 1-11 (2002).

[22] Daft, R.: Organization Theory and Design. 2nd ed. West, St. Paul, Minn. (1986).

[23] Wainer, J., Barthelmess, P., Kumar, A.: W-RBAC - A Workflow Security Model Incorporating Controlled Overriding of Constraints. International Journal of Cooperative Information Systems 12(4), 455-485 (2003).

[24] Oh, S., Park, S.: Task-Role Based Access Control (T-RBAC): An Improved Access Control Model for Enterprise Environment. In: Proceedings of the 11th International Conference on Database and Expert Systems Applications (DEXA '00), Greenwich, London, UK, 2000 (2000), http://dx.doi.org/10.1016/S0306-4379(02)00029-7