December 2006

A Procedure Model for Enterprise-Wide Authorization Architecture

Felix Wortmann
University of St. Gallen

Robert Winter
University of St. Gallen

A Procedure Model for Enterprise-Wide Authorization Architecture

Felix Wortmann
Institute of Information Management
University of St. Gallen
Felix.Wortmann@unisg.ch

Robert Winter
Institute of Information Management
University of St. Gallen
Robert.Winter@unisg.ch

ABSTRACT

A procedure model for the development of an authorization architecture, which spans different IT systems and organizational units, is presented. Based on a conceptual discussion of authorization and authorization architecture, existing approaches are discussed. As basic requirements for authorization architecture, a theoretical foundation and a transparent derivation of the procedure model and activities from successful industry practices are proposed. Actual industry practices are presented as case studies, and a procedure model is derived by consolidating these practices. Since the inductively derived procedure model claims reference model status, the paper concludes with a discussion of its genericity and recommendation character.

Keywords

Access Control, Architecture, Authorization, Procedure Model.

INTRODUCTION

A fundament prerequisite for ensuring the security of information systems is the appropriate administration and control of access rights (Rupprecht and Wortmann 2006). The associated activities, which are grouped together under the term "authorization" (Jonscher and Dittrich 1994, Pernul 1995, Samarati and de Capitani di Vimercati 2002), confront IT management with numerous challenges. In the past, inadequate architecture management led to redundancies or gaps in the system landscape (Winter 2003), particularly in the case of mid-sized and large enterprises. In the authorization environment, inadequate management means that the individual systems usually possess independent and therefore redundant modules which from the implementation perspective are nonetheless proprietary and mutually incompatible (Kern et al. 2002). Moreover, in the case of standard software there is virtually no other option than to use the system-specific authorization components. In practice, the administration and control of access rights are largely performed on a system-related basis due to the proprietary components, which means that cross-system transparency regarding access rights and an efficient administration can only be achieved to a limited degree (Kern et al. 2002). In particular, this lack of transparency stands in contradiction to increasing regulatory requirements (Hartje et al. 2003, Menzies et al. 2004, Robinson 2005), such as e.g. those imposed by the Sarbanes-Oxley Act (Congress of the United States of America 2002).

The goal of this paper is therefore to derive a procedure model which is aimed at developing cross-system and enterprise-wide authorization architectures for the medium and long-term planning and design of authorization infrastructures. As a first step, the fundamental principles of authorization are explained, and the elements of an authorization architecture discussed. Current approaches from the areas of authorization, architecture and security management are then investigated in respect of existing procedures for developing authorization architectures. This is followed by the identification of requirements which the procedure model to be developed will need to satisfy. Since existing approaches have provided little detail in respect of the focus of this paper, a procedure model is therefore derived inductively on the basis of selected case studies. Finally, the derived model is evaluated by means of the identified requirements.

AUTHORIZATION ARCHITECTURE

Authorization and Authorization Architecture

Authorization or its synonym access control (Pernul 1995) denotes the verification and administration of access rights (Rupprecht and Wortmann 2006). The verification of access rights is defined as the process of conveying queries to the resources and data of a system, and deciding whether a query should be accepted or rejected (Samarati and de Capitani di Vimercati 2002). The administration of access rights encompasses the granting, withdrawal and maintenance of access rights.

Key elements of the authorization architecture are (1) the authorization processes and (2) authorization components and their interaction. The authorization processes encompass the activities for the administration and control of access rights (Rupprecht and Wortmann 2006). Authorization components are software components which provide functionalities for the administration and/or control of access rights (Wortmann 2006). The concrete authorizations exist in the form of authorization concepts. An authorization concept encompasses the rules depicted in the information technology which define which user can access which methods and/or data objects (Wortmann 2006). A specific authorization concept encompasses system-specific rules. An enterprise-wide authorization concept encompasses cross-system rules.
An authorization architecture is specified by means of models, directives and lead elements:

- Models: Structural facts are depicted with the aid of differentiated, aggregated, static (architecture) models (Hafner 2005). These models of the overall context primarily serve the purposes of communication and coordination.
- Directives: In practice, widely varying terms such as "standards", "rules", "guidelines" or "instructions" are used in the context of directives (Hafner 2005). The goal of directives is to provide statements that can be applied to a total universe of problems which is as broad as possible (Hafner 2005).
- Lead elements: Although the design of an architecture primarily envisages the structuring of an information system, it also provides concrete artifacts when necessary (Birkhölzer and Vaupel 2003). The goal is to investigate individual design options for applicability, e.g. by specifying or developing concrete infrastructure components, and/or to provide key artifacts (Hafner 2005).
-

Measures which can be grouped together according to content aspects to form complexes of measures describe the implementation of the authorization architecture. Here, the models, directives and lead elements used to specify the architecture are to be assigned in particular to the organization architecture (sequence and responsibilities of authorization processes) and the IT architecture (technical structure of authorization infrastructures) (Wortmann 2006).

State of the Art of Authorization Architecture Development

For the purposes of this review, approaches were analyzed which can be utilized for the development of a suitable procedure model and thus (1) refer explicitly to the topics of authorization and architecture, (2) include or focus on a procedure model, (3) with regard to their level of abstraction allow sufficiently concrete discussion and (4) are implementation-oriented and/or have already been used in practice.

Approaches from the area of security management discuss procedures to ensure the security of information systems (A-SIT 2004). Many national [e.g. (BSI 2004)] and international [e.g. (ISO 1997)] standards describe the elementary activities of security management, but they only reveal little detail when it comes to the specific topic of authorization architecture.
Approaches from the field of cross-system authorization deal in particular with the structure and interaction of authorization components as well as with the associated design and development of authorization concepts. Here, the discussion centers on the one hand on the way in which key authorization components can be provided as infrastructure [e.g. (Kern et al. 2004)]. On the other hand, it focuses on whether and, if so, how the access rights of different authorization components can be integrated on a cross-system basis [e.g. (Roeckle et al. 2000, Kern et al. 2002, Kuhlmann et al. 2003). However, there is no emphasis on procedures for the medium and long-term planning of authorization infrastructures.

In summary it can be said that the approaches taken from the fields discussed provide little detail with regard to the main topic of this paper. In particular, there is a lack of sufficiently specific procedure models on which to draw for the development of authorization architectures. Moreover, a large proportion of the approaches are neither theoretically well-founded nor transparently derived from current practices. For this reason, empirical projects are presented in the following section in the form of case studies which subsequently provide the starting point for derivation of the procedure model. First of all, however, major requirements which must be met by the procedure model to be developed are derived and defined.

REQUIREMENTS TO BE MET BY THE DERIVED PROCEDURE MODEL

The procedure model is to be derived with aim of achieving reference model status. It must therefore satisfy the two typical properties of a reference model (vom Brocke 2003): reference models are *generic* under certain conditions defined in the model, i.e. they can be used for a category of applications. In addition, they possess *reference character*.

Genericity and Reference Character

Genericity denotes the extent to which a developed reference model can be used by different enterprises (vom Brocke 2003). The criterion of genericity is to be considered as critical, particularly from the constructivist perspective, since objective applicability does not exist in constructivist terms (vom Brocke 2003): the acceptance of a reference model results solely from the perception of the individual subject. Even if the genericity of a reference model can consequently only be achieved with limitations, the procedure model to be developed nonetheless lays claim to cross-industry genericity. In particular, it should be suitable for large enterprises which are characterized by heterogeneous, historically evolved application landscapes and therefore security landscapes.

The identification of structural analogies and/or patterns by means of induction constitutes an important starting point for satisfying the requirement for genericity (Schütte 1998). In this paper, the derivation of the procedure models takes the importance of induction into account and is based in particular on the generalization of case studies. During the course of development, however, a deductive and/or argumentative approach should also be adopted in order to support and extend the inductive findings.

The *recommendation character* of a procedure model encompasses the claim to possess exemplary properties in the sense of a reference procedure (Braun et al. 2005). Here, the verifiability of the recommendation content proves to be problematic (vom Brocke 2003). The question of whether recommendation character exists is not decided until the procedure model is applied and thus depends on its perceived suitability taking into account the specific circumstances of the case. For reference modeling, it is emphasized that the development of a reference model on the basis of a defined goal and/or requirements system is only possible within certain limitations as it is not possible to establish a generic goal system (Schütte 1998). The recommendation character of the procedure model to be developed can therefore only be ensured and proven to a limited extent on the basis of goals and requirements. In the context of this paper, the genericity of the requirements system is to be addressed by basing the derivation of the concrete requirements to be met by the procedure model, which is to be performed in the following section, exclusively on established security standards.

Requirements from Security Management

In recent years efforts have increased both at national and international level to develop harmonized procedures to ensure the security of information systems (A-SIT 2004). The explanations given below are based on the ISO/EIC Standard 13335 “Guidelines for the Management of IT Security“ (ISO 1997) as a harmonized method of this kind since it is widely accepted and deals in depth with the organization and implementation of security in the form of a code of practice (BITKOM 2005). The broad acceptance of this standard is attributable to the fact that many European countries were involved in its development.

Within the second part of the ISO standard, “Managing and Planning IT Security”, the activities of security management are described which are summarized as follows (A-SIT 2004):

- Development of a corporate IT security policy: The corporate IT security policy encompasses the guidelines and specifications which define the fundamental goals, strategies, responsibilities and methods for ensuring IT security.
- Risk analysis: A major task of security management is the recognition and assessment of security risks as well as their reduction to an appropriate level.
- Development of a security concept: On the basis of the identified risks, it is important to develop measures to reduce the residual risk to an appropriate level. In the case of complex IT systems, individual IT security policies should be developed which not only describe guidelines and specifications for the particular system but also concrete security measures and their implementation.
- Implementation of a security plan: Implementation of the measures developed must be accompanied by awareness-building and training activities. Moreover, it is important to make sure that the concrete implementations satisfy the guidelines and specifications which have been drafted (“accreditation”).
- IT security in continuous operation: Security management also includes the task of maintaining and if necessary adapting security in continuous operation.
-

The procedure model to be developed is dedicated to the conceptual development of authorization architectures, which means that the development activities of security management form the relevant starting point. The following requirements can be derived from the respective activities of security management:

Security Management Activity	Resulting Requirement	Description of Requirement
Development of a corporate IT security policy	Compliance with existing security guidelines and specifications	The development of a corporate IT security policy is not the object of the procedure model to be developed. This procedure must nonetheless comply with existing security guidelines and specifications.
Risk analysis	Performance of a risk analysis	Risks are to be systematically addressed when developing the procedure model.
Development of an IT security concept	Derivation of the appropriate measures	On the basis of the identified risks, appropriate measures must be derived to reduce the residual risk to an appropriate level.
	Definition of guidelines	In the case of complex IT systems, separate guidelines should be developed which constitute concrete procedural instructions.

Table 1: Requirements to be met by the Procedure Model

DERIVATION OF THE PROCEDURE MODEL

In order to ensure that the procedure model is derived transparently, two procedure models from the world of practice are first outlined in the next section. These were developed as case studies on the basis of interviews and document analysis. These cases were selected because the companies concerned had many years of experience-based know-how in the development and maintenance of security architectures. In addition, both companies had possessed an extensive security and authorization infrastructure for some time. The chapter concludes with an inductive derivation of the consolidated procedure model on the basis of these case studies.

Case Study A: Credit Suisse

The development and implementation of the present authorization architecture at Credit Suisse began in 2000, having identified improvement potentials in the granting of access rights according to the "need to know" principle. The "Position Paper on Access Control" in mid 2000 first provided an overview of the as-is status of authorization and on this basis developed the beginnings of a solution for the identified challenges. The conceptual work was then continued within the framework of two projects: the "authorization architecture" specified the to-be situation for authorization in the form of standards which stipulate the fundamental aspects of authorization. At the same time, the more comprehensive "security architecture" was developed which assesses the measures elaborated in the "authorization architecture". Figure 1 shows the main phases and activities for derivation of the authorization architecture, which are explained in greater detail in the next section. The broken line in Figure 1 indicates the iterative procedure: during the course of time the developed concepts were structured with an increasing level of detail.

The *development of fundamental principles* was performed at the start of the conceptual work. The security architecture model was developed within the framework of the security architecture (activity 1.1) in order to delimit and subdivide the universe of discourse of different security architectures. Development of the security architecture and authorization architecture was performed on the basis of internationally recognized standards. The standards were adapted to the needs of Credit Suisse in the respective documentation (activity 1.2). On the basis of the security standard ISO/IEC 17799, key security requirements were elaborated which needed to be taken into account in the proposed solutions (activity 1.3). Finally, key terminology was defined and compiled in the form of a glossary (activity 1.4).

Selected authorization components were analyzed in conjunction with *recording the as-is situation* (activity 2.1). Key components were evaluated amongst others according to the criteria "field of application", "database", "access rights" and "security check". Use of the individual authorization components is described under the heading "field of application". "Database" focuses on the data sets which are used as the basis for authorization checks. "Access rights" and "security checks" describe the fundamental authorization concept behind the respective components as well as the type and scope of existing rights. Existing as well as new authorization requirements were identified during its preparation (activity 2.2).

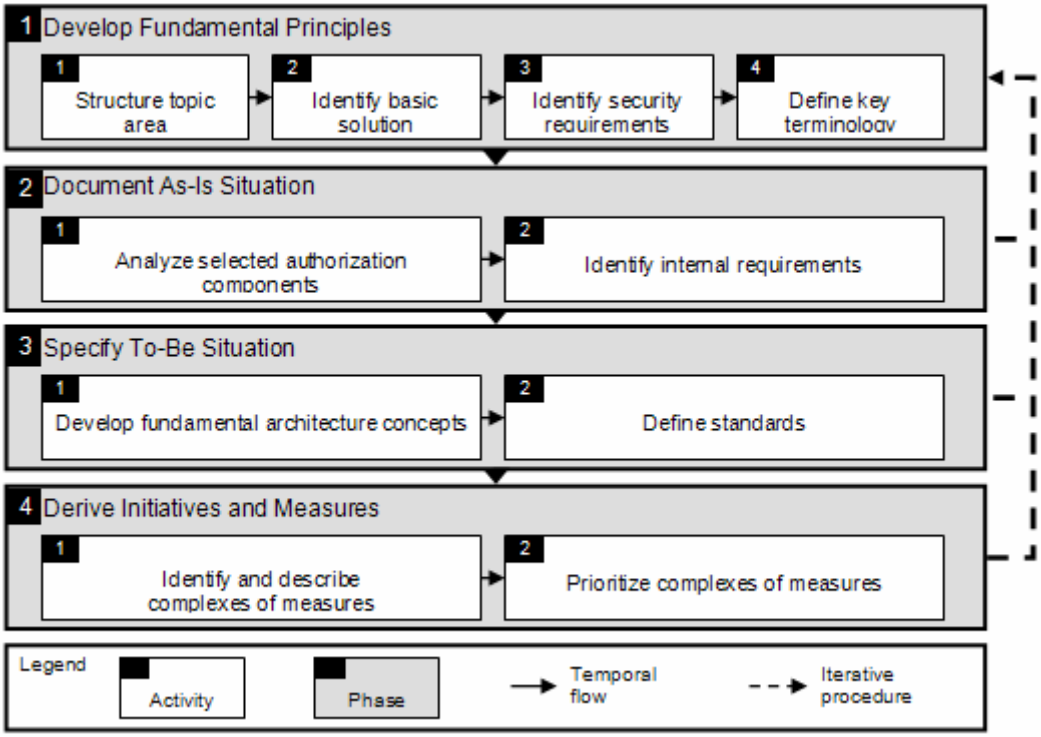

Figure 1. Credit Suisse Procedure Model

Definition of the to-be situation for authorization began as early as mid 2000 with the development of fundamental architecture concepts (activity 3.1) which were described in the form of medium and long-term solution scenarios. Finally, with the authorization architecture, the architecture department developed a detailed description of the to-be situation by defining standards (activity 3.2) which stipulate fundamental aspects of authorization. A summary of the to-be situation can be found in the roadmap of the security architecture.
The *derivation of initiatives and measures* for authorization encompassed the development complexes of measures (activity 4.1) in conjunction with the authorization architecture. The prioritization of these complexes of measures (activity 4.2) was then performed as part of the security architecture in the roadmap document. The costs of the complexes of measures and their benefits in the form of the anticipated security gain were used as evaluation criteria for this purpose.

Case Study B: Winterthur Group

The development of a comprehensive authorization architecture for Winterthur took place within the framework of two projects. The Winterthur project "CC AIM" produced the first approaches to a solution in the area of authorization in 2004. The "Winterthur Security Architecture" project in 2005 built on the work of the CC AIM project. Figure 2 shows the project procedure for deriving the authorization architecture at Winterthur. Once again, the main project phases and their activities are stated. A special feature of this project was the "define to-be situation" phase: these activities are performed in parallel with one another with permanent coordination. The broken line in Figure 2 again indicates the iterative procedure.

The first phase of the projects involved developing the *fundamental principles*. The topics of data protection and data security were used as the starting point for elaborating the question of authorization (activity 1.1). By investigating case studies and literature, the working group looked at initial concrete solution scenarios for Winterthur (activity 1.2). Requirements which have to be taken into account for authorization in heterogeneous system landscapes were then discussed in the light of international security standards (activity 1.3).

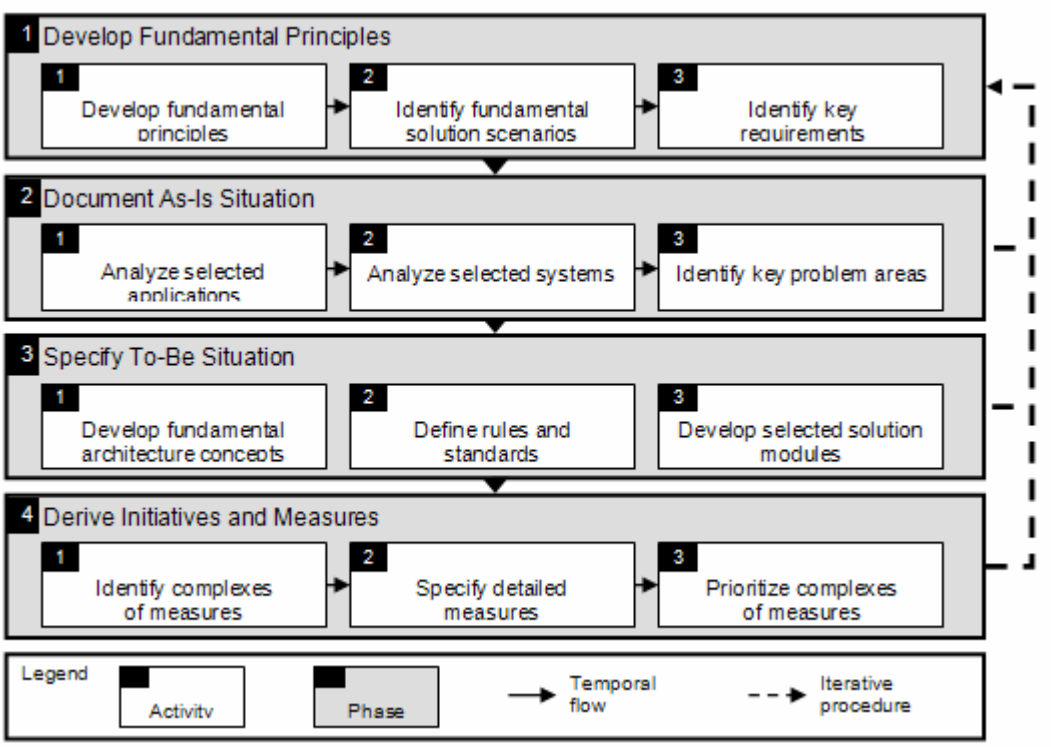

Figure 2. Winterthur Group Procedure Model

The *as-is situation* was analyzed on the basis of the requirements and solution scenarios discussed. Selected applications were investigated in respect of authorization (activity 2.1). In addition to the applications, the working group investigated and evaluated individual authorization components (activity 2.2). The analysis of the selected applications and systems concluded with the identification of key problem areas (activity 2.3).
Subsequent definition of the *to-be situation* involved developing fundamental architecture concepts (activity 3.1) which defined key responsibilities and rules within the framework of the selected architecture scenarios (activity 3.2) as well as defining and specifying selected solution modules (activity 3.3).
In the final phase, *initiatives and measures* were derived. Complexes of measures were identified on the basis of the determined improvement potentials and the elaborated target solutions (activity 4.1). The individual measures in these complexes were described and briefly characterized, the dependencies between measures documented and responsibilities assigned (activity 4.2). To conclude, the complexes of measures were prioritized (activity 4.3).

Derivation of the Consolidated Procedure Model

The induction of the consolidated procedure model consists of two steps and is based on the construction of reference models (Schütte 1998, Brocke vom 2003). First of all, the activities encompassing similar functional tasks are consolidated in the induced procedure model (cf. Figure 3).

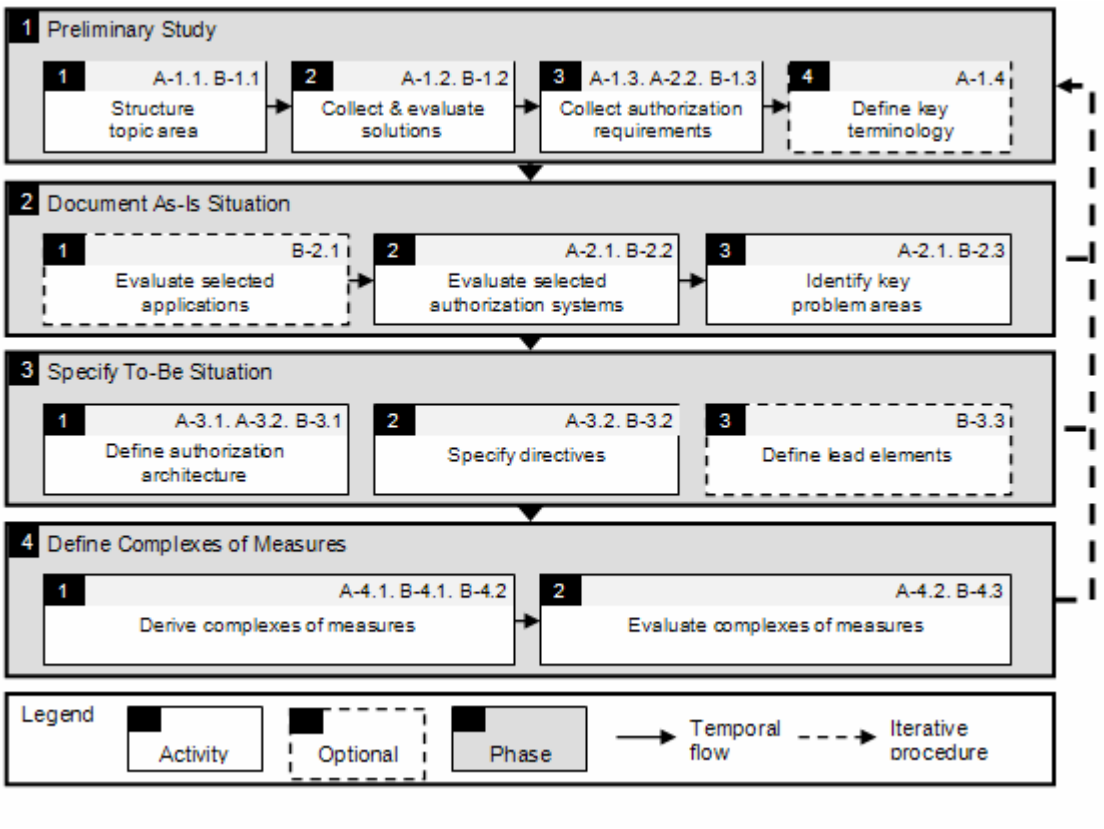

Figure 3. Derived Procedure Model

To ensure the transparency of the derivation the corresponding activities in the case studies are stated for each derived activity in the depicted procedure model. The results of the activities play a special role in the derivation. Activities with the same or similar results indicate functional units which are to be consolidated. In the figure, the activities have already been assigned to the induced phases. The derivation of the phases was performed analogously to the definition of activities by consolidating phases that comprise similar task units. Activities marked as "optional" only originate from one of the case studies analyzed.

Finally, the derivation of the procedure model is performed. The temporal flows between the phases and activities in the induced procedure model are defined on the basis of behavioral identities (Schütte 1998): similar activity sequences are consolidated in the induced procedure model. An overview of the individual phases with their activities is outlined in the following section.

The basic foundations for developing the authorization architecture are laid as part of the *preliminary study*. At the beginning of the phase it is important to delimit and subdivide the universe of discourse for the architecture to be developed (activity 1.1) in order to ensure complete development of the architecture with minimum overlap. Development of the authorization architecture can build on existing contributions from science and practice which are available e.g. in the form of literature or standards. These contributions must be collected and reviewed in accordance with the application context (activity 1.2). Security standards such as ISO 17799 stipulate that the requirements to be met by authorization must be collected and documented (ISO 2000). The requirements must thus be defined before the actual architecture itself (activity 1.3). To encourage the use of uniform language in the area of authorization it is advisable to introduce a glossary which defines and documents the specialist terminology employed (activity 1.4).

In the "*document as-is situation*" phase, weak points are determined which then serve as the starting point for development of the architecture. Selected authorization components are evaluated in order to ensure that the weaknesses of individual authorization components are adequately addressed (activity 2.2). Above and beyond this, it is advisable to analyze selected

applications with a view to identifying cross-system weak points in authorization (activity 2.1). Finally, the results of the preceding activities are consolidated: key problem areas are identified by clustering and weighting the weak points found (activity 2.3).

The goal of the "*specify to-be situation*" phase is to develop the main design options and procedural instructions for resolving identified problems. Essential aspects of the to-be authorization architecture are established by defining and selecting key design options (activity 3.1). Important solution principles on which the developed design options are based are recorded in writing and detailed in the form of directives (activity 3.2). In addition, individual design options are investigated for applicability by specifying or developing concrete infrastructure components (activity 3.3). Within the framework of the case studies it was shown that the activities in this phase are closely coordinated and performed in parallel.

The last phase, "*define complexes of measures*", involves identifying complexes of measures to implement the developed approaches. As a first step, measures must be derived on the basis of the results already obtained and bundled to form complexes of measures taking into account semantic correlations (activity 4.1). Finally, it is necessary to prioritize the complexes of measures identified and to check whether they ensure an appropriate reduction of the discovered risks (activity 4.2).

Evaluation of the Consolidated Procedure Model

The procedure model resulting from the preceding sections claims genericity and also aspires to achieve recommendation character. The extent to which the presented procedure model fulfills these two aspects is outlined in the following section. The identification of structural analogies provides an important basis for satisfying the requirement for *genericity* (Schütte 1998). An analysis of the case studies in respect of structural analogies highlights numerous commonalities. Both case studies reveal appropriate phases with corresponding core activities: development of the fundamental principles is the first step, followed by analysis of the as-is situation, then definition of the to-be situation. Finally, complexes of measures are derived on the basis of the activities performed. Thus, as with the approaches to security management, the procedure first envisages the identification and evaluation of existing weak points so that measures can subsequently be developed to eliminate weak points while considering the risks. As a consequence, the commonalities of the case studies can be explained in terms of content. This means that semantic structural analogies (Schütte 1998) exist which justify the claim of the consolidated procedure to genericity.

The *recommendation character* of the outlined procedure model can only be secured and proven with certain limitations (vom Brocke 2003). The requirements defined in section 3 for this purpose are addressed as follows by the inductively derived procedure model:

- Inclusion of existing guidelines and specifications: Within the framework of the induced procedure model, existing guidelines and specifications are included through the activity "collect authorization requirements" in the "preliminary study" phase.
- Performance of a risk analysis: In order to satisfy the principle of operational efficiency, existing weak points must be identified, evaluated and only then addressed in accordance with the risk. The induced procedure model tackles these aspects in the "record as-is situation" phase. Risks are identified by analyzing applications and systems and subsequently evaluated.
- Derivation of appropriate measures: On the basis of the identified risks, measures have to be derived which reduce the risks to an appropriate level. The induced procedure model takes these requirements into account in the phases "define to-be situation" and "define complexes of measures". The "define to-be situation" phase encompasses the activities for developing design options and guidelines. The "define complexes of measures" phase bundles measures which are necessary for implementing the design options to form complexes of measures. These are then evaluated to promote implementation of the complexes of measures with the best cost-benefit ratio.
- Definition of guidelines: In the case of complex IT systems, security standards envisage the development of guidelines which constitute concrete procedural instructions. This is the equivalent of developing directives, which is to be performed within the activity "specify directives".
-

Consequently, the induced procedure model addresses the requirements developed. However, the question of whether the requirements developed are adequately addressed will only be decided when the procedure model is applied and thus depends on the circumstances (vom Brocke 2003).

SUMMARY AND OUTLOOK

The aim of this paper is to derive a procedure model for the development of cross-system and enterprise-wide authorization architectures for the medium and long-term planning and design of authorization infrastructures. For this purpose, fundamental approaches to authorization were first explained and key elements of an authorization architecture discussed. Existing approaches to the development of a cross-system and enterprise-wide authorization architecture are not very detailed and are neither theoretically well-founded nor transparently derived from current practices. During the course of this paper, therefore, empirical projects in the form of case studies were presented which constitute the starting point for development of a procedure model. The subsequent, inductively derived procedure model aspires to reference model status. In this respect it was necessary to conclude by examining the extent to which the obtained procedure model fulfills the two aspects of "genericity" and "recommendation character".

The resulting procedure model encompasses the four phases "preliminary study", "record as-is situation", "define to-be situation" and "define complexes of measures". The preliminary study involves laying the basic foundations (e.g. structuring the topic area, collecting requirements) for the development of an authorization architecture. In the "record as-is situation" phase, weak points are identified and serve as the starting point for architecture development. The goal of the "define to-be situation" phase is to develop essential design options and procedural instructions to resolve the identified weak points. Finally, in the last phase, "define complexes of measures", complexes of measures are identified to implement the developed approaches.

Further research work should be aimed at validation of these results on the basis of broader-scale case studies. Moreover, it would be advisable to further refine the procedure model in order to obtain detailed procedural instructions for individual activities. The developed model could also be integrated into existing approaches in architecture and security management.

REFERENCES

1. A-SIT (2004). Österreichisches IT-Sicherheitshandbuch – IT-Sicherheitsmanagement, http://www.a-sit.at/unterstuetzung/sicherheitshdb/OE-IT-SIHB_V2_2_Teil1.pdf, last accessed on 2005-02-17
2. Birkhölzer, T.Vaupel, J. (2003). IT-Architekturen – Planung, Integration, Wartung. Berlin: VDE.
3. BITKOM (2005). Kompass der IT-Sicherheitsstandards, http://www.bitkom.org/files/documents/BITKOM_Broschuere_Sicherheitsstandard_V1.01f.pdf, last accessed on 15.07.2005
4. Braun, C. and Wortmann, F. and Hafner, M.Winter, R. (2005). Method Construction – A Core Approach to Organizational Engineering, Santa Fe, 1295-1299.
5. Brocke vom, J. (2003). Referenzmodellierung – Gestaltung und Verteilung von Konstruktionsprozessen. Berlin: Logos.
6. BSI (2004). IT-Grundschutzhandbuch, http://www.bsi.de/gshb/deutsch/menue.htm, last accessed on 17.02.2005
7. Congress of the United States of America (2002). The Sarbanes-Oxley Act of 2002, http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf, last accessed on 2005-12-06
8. Hafner, M. (2005). Entwicklung einer Methode für das Management der Informationssystemarchitektur im Unternehmen, Dissertation, Universität St. Gallen, St. Gallen, 2005
9. Hartje, H. and Probst, U. and Jäck, K.Hessler, M. (2003). SAP Berechtigungswesen – Design und Realisierung von Berechtigungskonzepten für SAP R/3 und SAP Enterprise Portal. Bonn: Galileo Press.
10. ISO (1997). ISO/IEC TR 13335-2 – Guidelines for the Management of IT Security – Managing and Planning IT Security, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21755&ICS1=35&ICS2=40&ICS3=&scopelist=, last accessed on 2005-08-12
11. ISO (2000). ISO/IEC 17799 – Code of Practice for Information Security Management, http://www.iso.ch/iso/en/prods-services/popstds/.../fr/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35, last accessed on 2004-03-01
12. Jonscher, D.Dittrich, K. (1994). Realisierung von Sicherheitsstrategien mit Hilfe flexibler Zugriffskontrollmechanismen. In: Bauknecht, K.Dittrich, K. (eds.). Sicherheit in Informationssystemen. Zürich: vdf, 23-52.
13. Kern, A. and Kuhlmann, M. and Kuropka, R.Ruthert, A. (2004). A Meta Model for Authorisations in Application Security Systems and Their Integration into RBAC Administration, Yorktown Heights, 87-96.

14. Kern, A. and Kuhlmann, M. and Schaad, A.Moffett, J.D. (2002). Observations on the Role Life-Cycle in the Context of Enterprise Security Management, Proceedings of the 7th ACM Symposium on Access Control Models and Technologies, Monterey, 43-51.
15. Kuhlmann, M. and Shohat, D.Schimpf, G. (2003). Role Mining – Revealing Business Roles for Security Administration Using Data Mining Technology, Proceedings of the 8th ACM Symposium on Access Control Models and Technologies, Como, 179-186.
16. Menzies, C. and Martin, A. and Jourdan, C. and Koch, M. and Strohm, A.Heinze, T. (2004). Sarbanes-Oxley Act. Stuttgart: Schäffer-Poeschel.
17. Pernul, G. (1995). Information Systems Security – Scope, State-of-the-art and Evaluation of Techniques. *International Journal of Information Management*, **15** (3), 165-180.
18. Robinson, T. (2005). Data Security in the Age of Compliance. *netWorker*, **9** (3), 24-30.
19. Roeckle, H. and Schimpf, G.Weidinger, R. (2000). Process-Oriented Approach for Role-Finding to Implement Role-Based Security Administration in a Large Industrial Organization, Proceedings of the 5th ACM Workshop on Role-Based Access Control, Berlin, 103-110.
20. Rupprecht, J.Wortmann, F. (2006). Zugriffskontrolle in heterogenen Applikationslandschaften. In: Schelp, J.Winter, R. (eds.). Integrationsmanagement. Berlin: Springer, 123-168.
21. Samarati, P.de Capitani di Vimercati, S. (2002). Access Control – Policies, Models and Mechanisms. In: Focardi, R.Gorrieri, R. (eds.). Foundations of Security Analysis and Design – Tutorial Lectures. Berlin: Springer, 137-196.
22. Schütte, R. (1998). Grundsätze ordnungsmässiger Referenzmodellierung. Wiesbaden: Gabler.
23. vom Brocke, J. (2003). Referenzmodellierung – Gestaltung und Verteilung von Konstruktionsprozessen. Berlin: Logos.
24. Winter, R. (2003). An Architecture Model for Supporting Application Integration Decisions, Neapel,
25. Wortmann, F. (2006). Entwicklung einer Methode für die unternehmensweite Autorisierung, Dissertation, Universität St. Gallen, St. Gallen, 2006