

# Role and process manager on the basis of a logical set of rules



## Critical comment on the state of technology

Most of the role models, available on the market, represent a static approach, which meets with the limits of a realistic use quite soon. Such limits are e.g.

- A too extensive number of roles
- No differentiation of job and system roles, making difficult the modelling of processes
- No possibility of considering dynamic structures ( team or project organisation)
- Only rudimental or no set of rules at all for control of the processes
- No regular coexistence of role-based and direct allocation of rights
- No multidimensional management of rights

How can a professional approach look like in reality to resolve these conflicts?

## Role and process model as a consistent concept

The author has come upon exactly these issues within the scope of his project work (approx. 10 years) and has developed suitable procedures in order to achieve a significantly higher quality of role modelling.

Over the years, the following methods have been developed and exemplarily realized in a system (**bi-Cube**<sup>®</sup>) in order to investigate the practicability of the particular solution:

- Integration of role modell and process control
- Adaptive role model
- Model inherent rules and inference machine
- Generic process models
- Security classification
- Referenced roles

In the course of an iterative process (process development  $\leftrightarrow$  Validation in real operation), the particular solutions have had to be permanently improved, however, which leads to the postulate that a logical model of an IPM (Identity & Provisioning Management) solution can only be developed to an efficient system in cooperation with developers, system architects and professional project managers.

### Integration of role model and process control

In order to adequately represent the factually existent coherences in the model, process controls have to be defined at the role already, such as the following:

- Kind of allocation (automatically or with release)
- Kind of application (by user, by superior only, ...)
- Release procedures (multi-stage, second set of eyes, accidental)
- Min - Max Control
- Criticality (business critical or irrelevant)
- Security Classification

All these so-called PX Controls defined at the role, influence the process manager significantly. Moreover, the role change process has to be controlled reasonably. Here, restriction to the role owner and additional security through password integration may be required and should be provided.

### Adaptive role model

A logically separate draft of the role model without considering the process control leads to a static model and consequently to an explosion of the number of roles on the attempt to consider the diversity

## Role and process manager on the basis of a logical set of rules



of reality all the same. Therefore, the **bi-Cube**<sup>®</sup> system provides for a differentiation of the system attributes into authority and technical attributes. The authority attributes of a target system in the role are to be defined as obligatory. Hence, specific but essential characteristics of system attributes (data stock, server, particular skills of the users, ...) are classified as technical attributes and have to be provided by the particular owners during the assignment (application procedure). This approval process can be multi-stage ( data owner, licence administration, cost officer, system engineer, ...) with each actor contributing specific attributes. Thus the role model is considerably relieved and the number of roles kept manageable.

### Differentiation of job and system roles

Job roles exclusively specify the task of the role owner, whereas the system roles determine the allocation of rights to a role. This distinction proved to be essential because:

1. The system roles comprise the specific system rights and are centrally determined
2. The job roles are defined as well as allocated in the departments.

Thus the aim of a central modelling and decentral administration is definitely achieved. Subject of the process management are the job roles only.

### Segregation of duties

Too, secure separation of objectionable competences is realized on the job role level most easily.

### Team and project organisation

A project-related role model is at least two dimensional (functional rights, data views). With a static role model this  $m \times n$  matrix would lead to an  $m \times n$  role model and finally to an absurd, not controllable, number of roles.

If the adaptive role model is applied to this problem, the number of roles is reduced to the number of the functional combinations of rights (Project manager, assistant, controller, engineer, ...). The particular views on the project data (project documents, file-space, mail group, ...) are procured during the role allocation in the process. Beyond, the problem of *segregation of duties* can be solved as only allowed combinations of data areas (different project documents) are offered for selection.

### Referenced roles

Another possibility of slenderizing the role model are the object references which can be defined on role and system level.

Object references are defined as so-called *advanced shared resources* (ASR). These are programs which are necessary as pre-condition for other programs (e.g. CICS- or DB-Client) and are bonded to the particular application on the system level already so that they do not have to be considered in the role model anymore.

In the same way, basic roles can be defined, which can be repeatedly bonded to job roles via object references so that they do not have to be defined in the actual job roles. A secondary effect: changes at the basic roles become easier and more secure.

### Generic process models (GPM)

For various processes in the provisioning, templates can be defined which reduce this sub-project by 70 to 80% in time and effort. These templates are tested in all parameters and can be used immediately in a productive environment.

In the GPM project of the iSM, a standard set of GPM was defined, explicitly described and realized in **bi-Cube**<sup>®</sup> step by step. Gradually, because this range of GPM is permanently expanded by new ideas originating from the projects.

## Role and process manager on the basis of a logical set of rules



The following processes have been identified from the operators point of view :

1. Application for the allocation of roles
2. Automatic allocation of rights for new employees (start of employment)
3. Confirmation and administration of policies (directives) - separately and integrated in the application process
4. Automatic withdrawal of rights of employees leaving the company (end of employment)
5. Immediate blocking of users
6. Consideration of sliding transitions / job change processes
7. Re-entrance into corporate group structures
8. General document-based application process
9. Request for general applications without structuring of rights
10. Support request to URA (user and rights administration )
11. Re-Licensing (regular confirmation of granted licences)
12. Re-Certification (regular confirmation of granted rights of use)
13. Re-Validation (regular confirmation of the existence of users)
14. Password self-service

### Secondary processes

- Application for a work place including equipment options
- Absence / holiday administration (for control of task-manager)
- Application for access rights

From these examples the following classification of IPM processes (into which all other processes may be integrated) can be derived:

### Process groups

- Job change processes of users
- Application procedures
- Repeat authorization
- Secondary processes
- Service processes
- Internal processes

### Model inherent rules and logic engine (inference machine)

The integration of roles and processes requires an efficient rule processing.

In IPM products (at least according to the knowledge of the author) there is only a complex of model inherent rules which are defined directly in the GUI to objects, attributes and the basic relations between them.

In the illustration below are shown 2 examples of this rule type in the **bi-Cube**<sup>®</sup> system.

A somewhat more complex rule definition with a rudimental Boolean logic can be found in the (user-) attribute - referencing of roles (chart 3). Thus the totality of defined roles is restricted in such a way that in fact only appropriate and reasonable competences can be assigned via roles.

It does not make sense to offer all roles from director to concierge to each user.

A further possibility is to define consequences which are based on the internal message protocol of **bi-Cube**<sup>®</sup>. Here each message is checked, whether there's a rule (consequence) for it or not. 4 combinations are possible:

If attribute 4711	Has value xy		Then attribute 3332	Set value to abc
If attribute 4711	Has value xy		Then start	Operation 1234
If operation	xyz		Then also start	Operation 1234
If operation	xyz		Then attribute 3332	Set value to abc

# Role and process manager on the basis of a logical set of rules

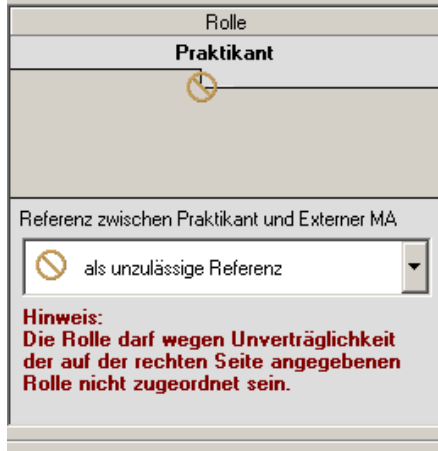


Chart 1

**FLAGLISTE**  
Flagliste

**1. Flag**

- Rolle ist genehmigungspflichtig
- Rolle ist nicht genehmigungspflichtig

**2. Flag**

- Rolle kann vom Leiter und vom User beantragt werden
- Rolle kann nur vom Leiter beantragt werden (Fremdantr)
- Rolle kann nur vom User beantragt werden (Eigenantra)
- Rolle kann automatisch beantragt werden

Chart 2

Top: rules for the control of the application processes  
To the right: Segregation of duties

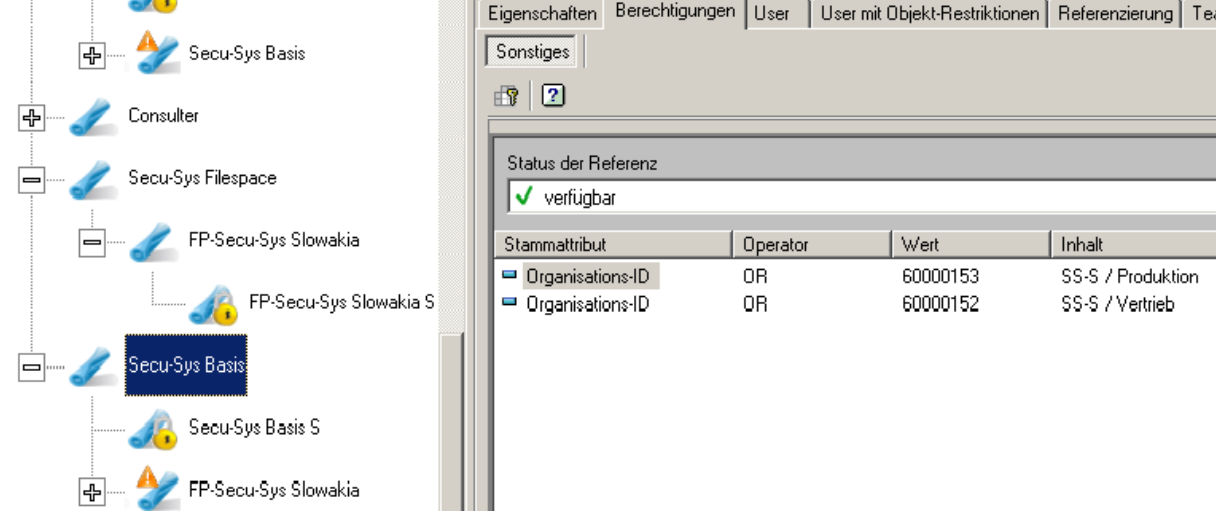


Chart 3

Stammattribut	Operator	Wert	Inhalt
Organisations-ID	OR	60000153	SS-S / Produktion
Organisations-ID	OR	60000152	SS-S / Vertrieb

The further qualification of the processes required more complex rules which could not be controlled anymore by the existent separate model inherent rules. E.g. the process “start of employment” is completely different for external users than for internal users.

Additional conditions (e.g. mandator dependencies) even increase the complexity of the process.

The simple way would have been to create individual modified process models for these special cases. However, this would not have solved the problem but only deferred the boundary of modelling.

Therefore a rule machine was developed and integrated for the processing of a logic engine (inference machine). These components (*bi-Cube*<sup>®</sup> - Logi) process simple, complex and also recursive Prolog-Notations. The chosen syntax has been designed in an almost natural language. Thus all occurring logical combinations for the process control can be framed and – after certain practice – be defined also by the operator.

## Coexistence of role and system authorizations

It is an accepted fact that the achievement of a completely role-based authorization is an evolutionary process, which will sooner or later or never be terminated.

Therefore there must also be a rule for the coexistence of direct and role-based authorization, as soon as both procedures collide.

This is the case, when an existent direct system authorization meets with a role-based one ( possibly

## Role and process manager on the basis of a logical set of rules



by migration). The general rule in this case is that the role-based authorization dominates the existing direct one, probably also withdrawing rights in this connection.

### Role conflicts

Definition: Role conflicts are the concurrence of different authorization profiles of a system of two (or more) roles. For this case there must be a rule for each system for an automatic dissolution of the conflict. Two typical rules are:

- Consolidation of both profiles on one account
- Creation of another account with the different profile

This rule has to be processed properly, also on multiple occurrence of such a conflict and - above all – on withdrawal of a role.

### Security Classification

It has proved to be reasonable that all objects and attributes can be provided with a Security Classification (SC). This SC is considered as another dimension of rights within the IPM set of rules. This set of rules can be used for the pre-selection of allocations. E.g. the user must have at least the same (or a higher) Security Class, like the required role. Moreover, certain actions can be made dependent on the SC of the role or the user. E.g. as from a defined SC level, another authorization or information to certain persons (e.g. security team) can be generated. Moreover, the SC is an important criterion within the internal control system (ICS).

## Summary

In this manuscript, various control possibilities within the role and process manager were demonstrated which all contribute to an improved modelling ability of real requirements. Depending on the efficiency of the set of rules, a product is in a position to reach a high IPM process level.

General cognition of all work was:

**Role model and process manager must realize a narrow integration with each other, what an efficient set of rules is indispensable for.**