

# Dynamical Identity Management in the Project Organization with *bi-Cube*<sup>®</sup>



## Table of contents:

1	OBJECTIVE.....	2
2	SPECIFICATIONS AND MODEL APPROACH .....	2
2.1	Requirements for the Role Model.....	2
2.2	Functions at the Team Organization.....	5
3	TEAM MANAGEMENT.....	6
4	INTEGRATION OF SKILL MANAGEMENT .....	7

## 1 Objective

All previous Identity Management (IdM) approaches are focused more or less on static structures in a company. In most cases the individual authorizations derived of an organizational structure. Neither the specific group policies in Active Directory, nor rule based assignments of rights in IdM solutions, related to management and organizational structures, have often no longer dominant influence on activities and tasks of the employees.

Especially in technology or manufacturing companies, cross-structured teams or project groups are combined, which often only exist at specified time intervals. This form of a more dynamic work organization calls for additional demanding requirements to the identity management. Due to the results of these requirements a methodical solution (in use) has been further qualified.

## 2 Specifications and Model Approach

### 2.1 Requirements for the Role Model

Customary roles are unsuitable for a team or a role based provisioning. For example:

10 team roles defined for 200 projects, considering project based data view, shape a value of 2000 roles. These roles have to be constantly managed because each new or completed model needs to be customized to the roles. This approach is not the idea of a simplified authorization structures.

As the principle of a project based role model, two requirements are to be considered:

1. Available solution, which supports project based data views without a multiplicity of roles.
2. This solution must consider the dynamics in the project organization by automatic processes, without having to constantly create project folder or project databases or similar objects.

### Dynamics in Team Roles

The rule based combination of roles and process models allow the defining of necessary team roles, including authorizations without indicating specific project rights (data views) in the role.

In the process of assigning a team role to a user these rights are generic determined and considered at the authorization structure of the role.

# Dynamical Identity Management in the Project Organization with *bi-Cube*<sup>®</sup>



This requires the following:

1. Referencing attributes of the project with authorization objects in the target systems will make it possible to create a file space as project data memory, to generate a project mail group and to manage project specific documents in the DMS. By entry of project specific key words, automatic links to databases such as in Notes and DMS systems are provided.
2. At role allocation, are for these three predefined objects adequate rights to the team assigned.
3. If required, additional rights of other target systems may be included to team roles by technical attributes and with additional properties must be obligatory attributes. These are selected by the user during the role allocation process.

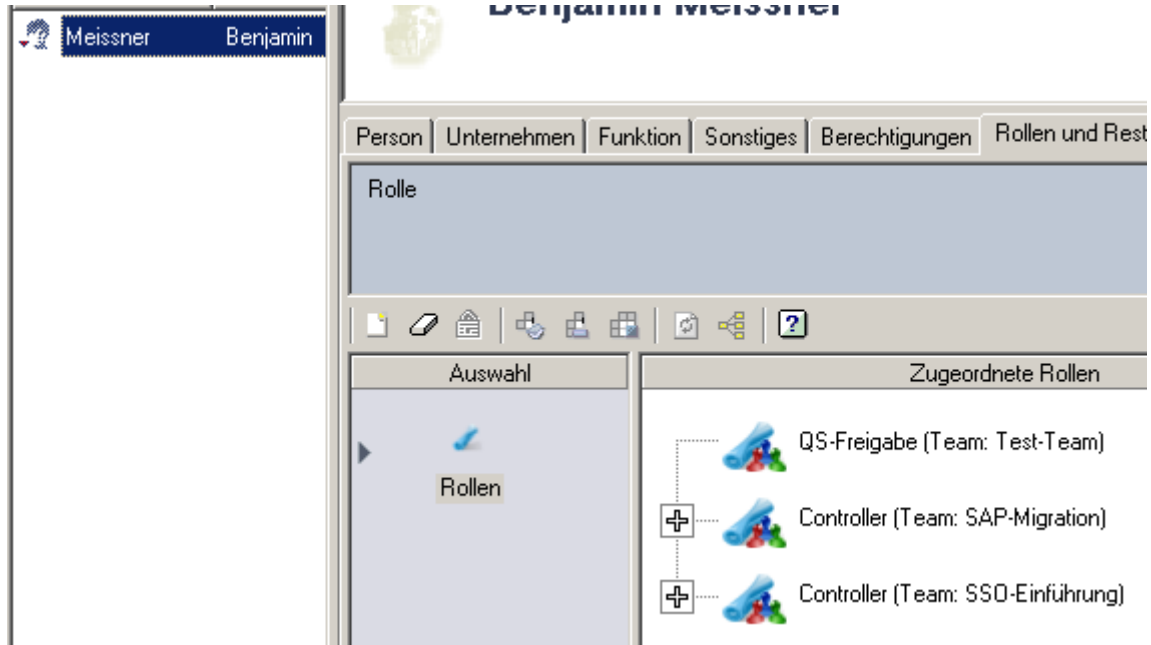
By these specific functions at the role and process management, the dynamics of the project organization in relation to the authorization structures can be fully met.

The screenshot displays the 'Test-Team' configuration page. On the left, a tree view shows the hierarchy: Team > IT-Projekte > Test-Team. The main area is titled 'Beschreibung ausgewähltes Team' and 'Test-Team'. It features a description field and several tabs: 'Eigenschaften', 'Mitarbeiter', 'Mitarbeiter Extras', and 'Kostenstellen'. The 'Eigenschaften' tab is active, showing fields for 'Teamart' (Projekt-Teams), 'Beginn' (18.06.2008), and 'Geplantes Ende' (18.07.2009). Below these are buttons for 'Projekt ändern' and 'Projekt beenden'. Further down, there are fields for 'Authentifikation', 'Kurzname' (11663. Objekt), 'Organisationseinheit' (Wählen... 00000010, EDV - Abteilung), 'Projektspezifische Datenbank' (Test-Team), and 'Dokumentkürzel' (Test-Team). At the bottom, there is a section for 'Weitere Eigenschaften' with a sub-section for 'ADS Eigenschaften' containing 'Dynamische Laufwerke'.

Screen shot 1: Project creation by the project coordinator

## Multi allocation of Team Roles

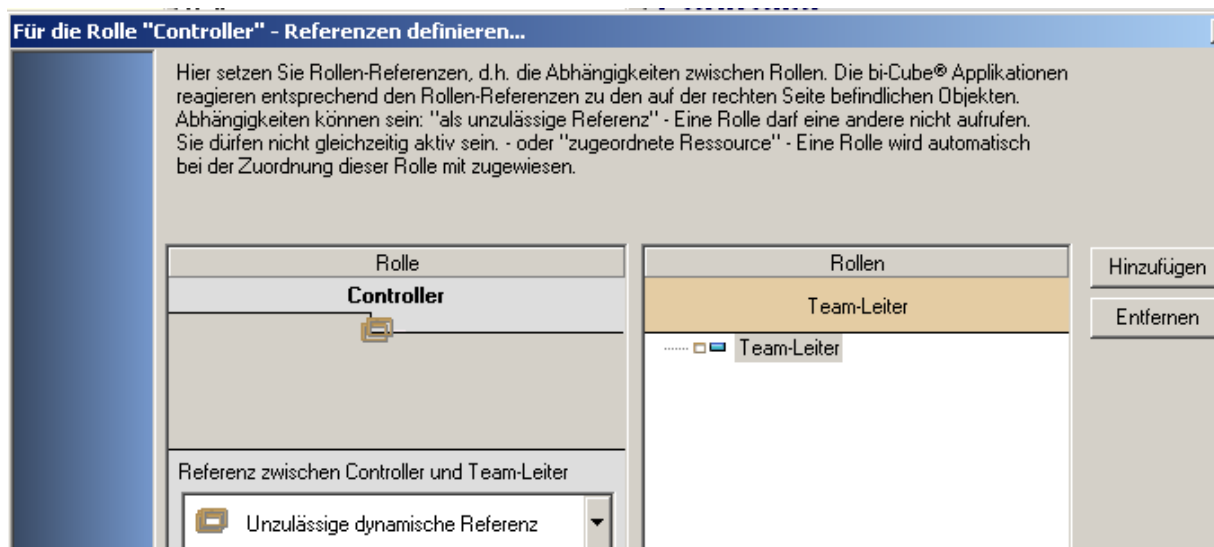
Several team roles may be assigned to one user. The user could be the supervisor or employee of multiple teams. This characteristic allows for the cancellation of  $m * n$  dimensions (m-roles and n projects), to the one dimension of the m-team-role. (See screen shot 2)



Screen shot 2: Multi allocation of same team roles to different projects

## Dynamical Separation of Duties

In addition to the normal rules and regulations of the definition of inadmissible role combinations and thus prohibited links of rights (static Separation of Duties), is at the role model for the teams the dynamical Separation of Duties to be considered. It will avoid inadmissible role combinations within one team, but permits them in diverse projects. E.g. A user may not be the supervisor and controller of one team, but in diverse projects this combination is possible.



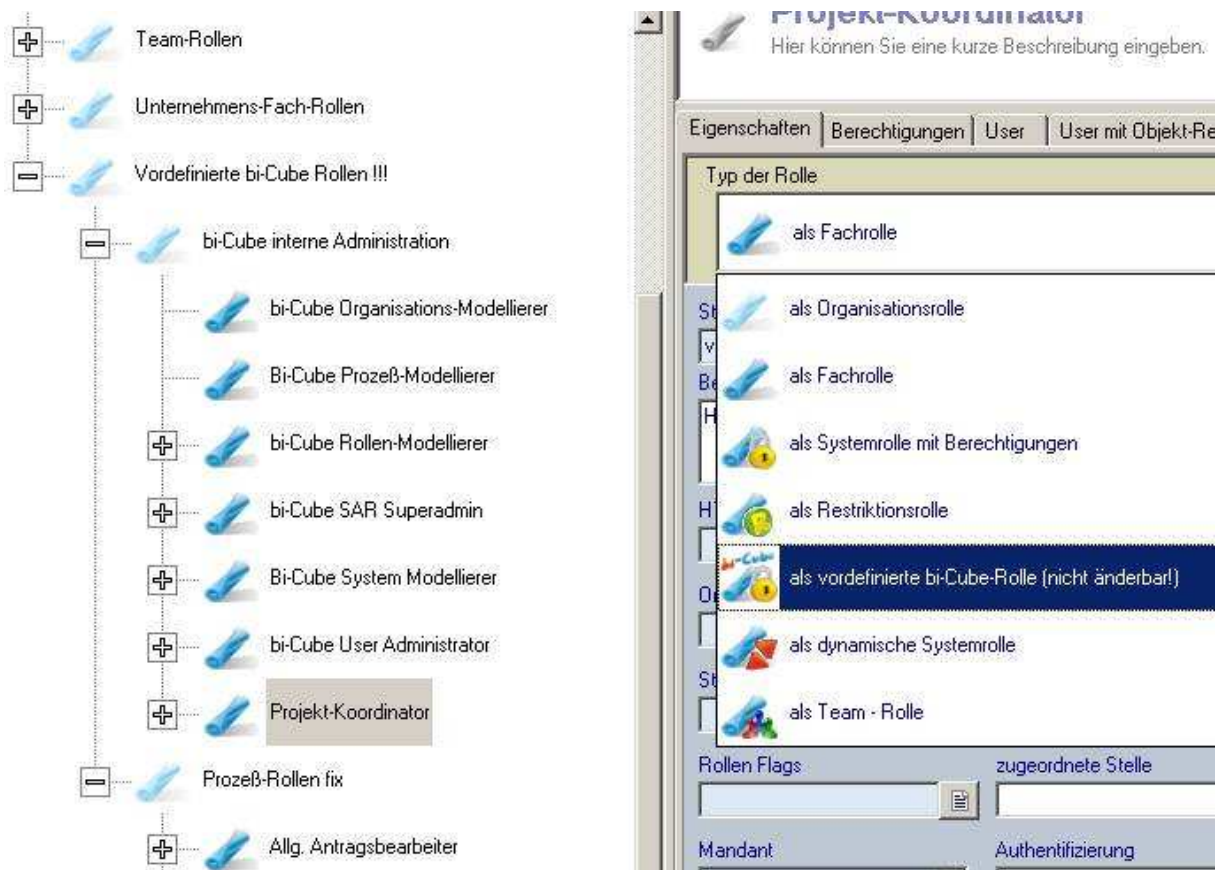
Screen shot 3: Definition of a dynamic Separation of Duties

## 2.2 Functions at the Team Organization

Supposedly at this model approach, additional team project coordinators exist, which have the following duties:

1. Initialization of a new project with the key data, such as duration of the project or ending date, classification level, possibly addition of clients and responsible organizational units.
2. Predefining key words based on project documents and databases.
3. Allocation of cost center for effort bookings of team members.
4. Appointing team members and leaders.

The project coordinators receive the exact predefined role with rights, allowing them to execute this function at the IdM. Thus they receive an overview of all projects, and with the assignment to several projects, reduce the burden of individual employees. The coordinator controls the duration of projects.



Screen shot 4: The project coordinator as a predefined role in the system

## 3 Team Management

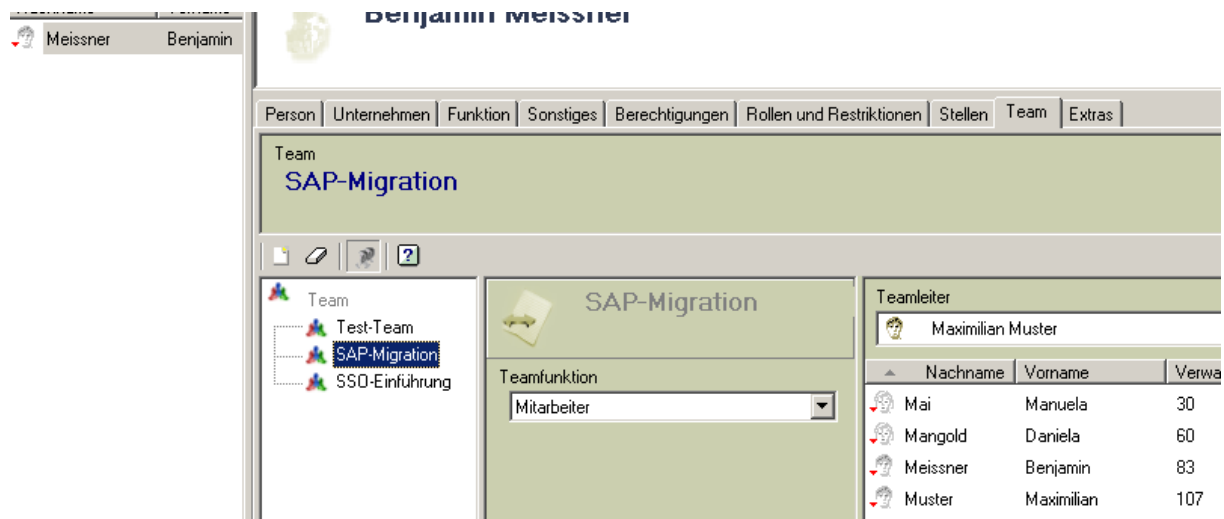
Team memberships of teams are managed by predefined generic processes. For entry and exit of the team by the user are for each, two process layouts implemented:

### Direct appointment of a user to a team

The project coordinator may directly appoint a user to a team. This is executed at the admin client with the following information:

1. Info to the user of his membership to the team, and that the user XY is his team leader.
2. Info to the team supervisor of an employee being appointed to a team.

Only this information is included, no authorizations are available and the process cannot be declined or reversed.



Screen shot 5: Direct appointment to a team

### Team membership request

Alternatively, user may function as actuator and request a team membership at the IdM Web Portal as follows:

- The project coordinator makes the request to the supervisor of a user and he may decline or approve, or
- the supervisor makes the request to the project coordinator who may also decline or approve, or
- the team leader makes the request, being declined or approved, first by the project coordinator and then by the supervisor. If the project coordinator declines the request, then the process is canceled. If the team leader is also the supervisor of the user, then of course there is no need for a supervisor's approval.

Every request should point out which role is intended for the user. Also the validity time period needs to be indicated. The request has to display the user's project involvement on a percentage basis. Also a free text field for comments is added to the request.

After required approval procedure, the user will be a team member and receive a role with possibly an ending date. All parties concerned, will be informed.

# Dynamical Identity Management in the Project Organization with *bi-Cube*<sup>®</sup>



## Direct dismissal of the user from the team

This process is to be executed only by the project coordinator.

## Request of dismissal from the team

The request can be made at the IdM Web Portal by the following persons:

1. The user himself (approval by 2. and 3.)
2. The supervisor (approval by 3.)
3. The team leader (approval by 2.)

The team data of the user and a free text field for comments is part of the request. All parties concerned, will be informed.

## Overview at the IdM Web Portal

Every authorized user may access the IdM Web Portal to view current projects, including their members and roles and also the project costs.

The screenshot displays the 'bi-Cube IPM Web' interface. At the top, there is a navigation bar with tabs for 'Service Center', 'Dokserver', 'SOP-Tools', 'Compliance', 'Telefonbuch', 'Hilfe', and 'Akt'. Below this, the user's session information is shown: 'Username: y000003' and 'Sitzung endet in: 44:21 min'. The main content area is divided into three columns. The left column, 'Service Center', contains a list of services such as 'Web Kennwort ändern', 'LAN Account Service', 'Objektverwaltung', 'Abwesenheiten', 'Userverwaltung', 'Antrag stellen', 'Task-Manager', 'Info-Übersichten', 'Vertragsverwaltung', 'Ressourcen', 'Interne Kostenverrechnung', 'Skill Management', and 'Teamverwaltung'. The middle column, 'Teamübersicht', shows a tree view of teams under 'IT-Projekte', including 'IDM-Einsatz', 'SAP-Migration', 'SSO-Einführung', and 'Test-Team'. The right column, 'Teammitglieder', lists 'Markert, Anton' and 'Meissner, Benjamin'. The bottom right section, 'Team-Rollen des Users', lists roles for different teams: 'Team: SAP-Migration' (Controller (Info)), 'Team: SSO-Einführung' (Controller (Info)), 'Team: Test-Team', and 'QS-Freigabe (Info)'.

Screen shot 6: General information platform of projects (subject to authorization)

## 4 Integration of Skill Management

An efficient IdM system will allow the integration of a skill management. For roles, the requirement level of certain skills is defined. At the user role (also a team role) allocation process, the requestor and the approver may prior to his task completing (request or release), check to what extent the user complies with the role requirements.

# Dynamical Identity Management in the Project Organization with *bi-Cube*<sup>®</sup>

Details zur Rolle: UHD - Windows Internet Explorer

Skillmanagement

ID der Rolle	Name der Rolle	Skill	1	2	3	4	5	6	7	8	9
10904	UHD										
		1 Teamfähigkeit	■	■	■						
		1 Leistungsfähigkeit	■	■							
		1 Engagement	■	■							
		1 Management	■	■							
		1 Kundenorientierung	■	■	■						
		1 Stressresistenz	■	■	■	■	■				
		1 Englisch	■	■	■	■	■				
		1 Allg. IT-Fachwissen	■	■	■						
		1 DB-Administrator	■	■							
		1 ADS	■	■							
		1 Betriebswirtschaft	■	■							

Screen shot 7: Comparison of the role request (green) towards the user's performance. Deficits are displayed in red.

With the support of this methodology it is possible to search for adequate team members within the entire company. The skills may be defined optional. The displayed skills (screen shot 7) are supplemented with e.g. training courses, certificates etc.

So called "K.O. skills" may also be defined for certain roles. For example, to receive this certain role a team leader or QS manager has to supply specific certificates.