

Dynamisches Identity Management in der Projektorganisation mit *bi-Cube*[®]



Inhalt:

1	ZIEL	2
2	VORGABEN UND MODELLANSATZ	2
2.1	Anforderungen an das Rollenmodell	2
2.2	Funktionen in der Teamorganisation	5
3	TEAM-VERWALTUNG	6
4	INTEGRATION DES SKILL-MANAGEMENTS	8

1 Ziel

Alle bisherigen IdM-Ansätze richten sich auf mehr oder weniger statische Strukturen in Unternehmen. In den meisten Fällen werden die individuellen Berechtigungen von der Aufbauorganisation abgeleitet. Ob das spezifische Group-Policies im Active Directory oder regelbasierte Zuordnungen von Rechten in IdM-Lösungen sind, sie beziehen sich auf Leitungs- und Organisationsstrukturen, die vielfach nicht mehr den dominierenden Einfluss auf Tätigkeiten und Aufgaben der Mitarbeiter haben.

Vor allem in technologieorientierten oder produzierenden Unternehmen werden strukturübergreifende Teams bzw. Projektgruppen zusammengestellt, die oft nur in einem definierten Zeitintervall existent sind. Diese Form der doch mehr dynamischen Arbeitsorganisation stellt andere und vor allem anspruchsvollere Anforderungen an das Identity Management.

Dies verlangt eine methodische Lösung, die sich im realen Einsatz bereits bewährt hat und die sich auf Grund dieser resultierenden Anforderungen im Einsatz, weiterhin qualifiziert.

2 Vorgaben und Modellansatz

2.1 Anforderungen an das Rollenmodell

Wenn man versucht, die üblichen Rollenmodelle auf den Bereich der Projektorganisation anzuwenden, kommt man schnell zu der Erkenntnis, dass diese Rollenmodelle für ein team- und rollenbezogenes Provisioning ungeeignet sind. Ein einfaches Beispiel mag dies verdeutlichen:

Wenn z.B. 10 Team-Rollen definiert wurden und diese auf 200 Projekte zu beziehen sind, kommt man unter Beachtung der projektbezogenen Datenansichten auf 2000 Ausprägungen von Rollen. Diese Rollen müssten dann auch einer ständigen Pflege unterliegen, da jedes neue bzw. abgeschlossene Modell eine Anpassung der Rollen erfordern würde. Ein solcher Ansatz widerspricht dem Grundgedanken eines jeden Rollenmodells, der eine Vereinfachung der Berechtigungsstrukturen und nicht diese Vervielfachung zum Ziel hat.

Es sind also zwei Anforderungen als Grundsatz eines projektbezogenen Rollenmodells zu berücksichtigen:

1. Es muss eine Lösung gefunden werden, die die projektbezogenen Datensichten ohne eine Vervielfachung der Rollen berücksichtigt
2. Diese Lösung muss durch automatische Prozesse die Dynamik in der Projektorganisation berücksichtigen, ohne ständig Projektordner bzw. Projektdatenbanken oder ähnliche Objekte anlegen zu müssen.

Dynamik in Team-Rollen

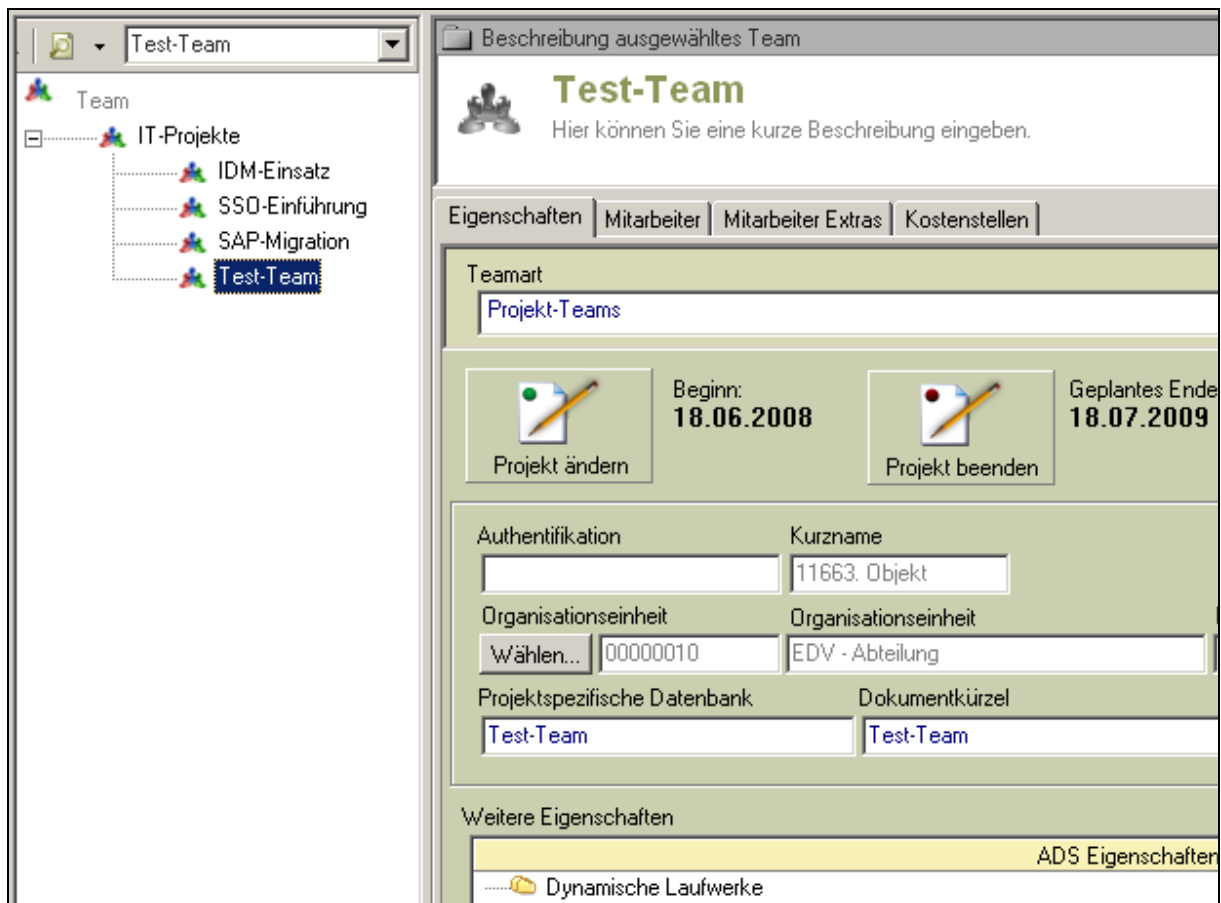
Die regelbasierte Verbindung von Rollen- und Prozessmodellen ermöglicht es, ausschließlich die erforderlichen Team-Rollen mit ihren Berechtigungen zu definieren, ohne in der Rolle die konkreten Projektrechte (Datensichten) angeben zu müssen.

Diese werden im Prozess der Zuordnung einer Team-Rolle zu einem User generisch ermittelt und in der Berechtigungsstruktur der Rolle berücksichtigt.

Dies setzt Folgendes voraus:

1. eine Referenzierung von Attributen des Projektes mit Berechtigungsobjekten in den Zielsystemen der Projekte erlaubt es, u.a. einen Filespace als Projekt-Datenspeicher anzulegen, eine Projekt-Mailgruppe zu generieren und im DMS projektspezifische Dokumente zu verwalten. Durch den Eintrag projektspezifischer Schlüsselworte werden automatisch die Verbindungen zu Datenbanken (z.B. in Notes und DMS-Systemen) geschaffen.
2. Für diese drei vordefinierten Objekte werden dann bei der Rollenzuteilung dem Team-Mitglied die entsprechenden Rechte zugeteilt.
3. Wenn es erforderlich ist, weitere Rechte anderer Zielsysteme in die Team-Rollen einzubeziehen, kann dies durch technische Attribute erfolgen, die an der Rolle nicht vorbelegt werden müssen aber durch die zusätzliche Eigenschaft ein Zwangsattribut zu sein, während des Zuordnungsprozesses der Rolle durch den Beantragenden ausgewählt werden können (bzw. müssen).

Durch diese spezifischen Funktionalitäten im Rollen- und Prozessmanagement kann der Dynamik der Projektorganisation in Bezug auf die Berechtigungsstrukturen voll entsprochen werden.



The screenshot displays the 'Beschreibung ausgewähltes Team' (Description of selected team) window for 'Test-Team'. On the left, a tree view shows the hierarchy: Team > IT-Projekte > Test-Team. The main area contains the following fields and controls:

- Teamart:** Projekt-Teams
- Beginn:** 18.06.2008
- Geplantes Ende:** 18.07.2009
- Buttons:** Projekt ändern, Projekt beenden
- Authentifikation:** [Empty field]
- Kurzname:** 11663. Objekt
- Organisationseinheit:** Wählen... 00000010
- Organisationseinheit (dropdown):** EDV - Abteilung
- Projektspezifische Datenbank:** Test-Team
- Dokumentkürzel:** Test-Team
- Weitere Eigenschaften:** ADS Eigenschaften, Dynamische Laufwerke

Abbildung 1: Anlage eines Projektes durch den Projekt-Koordinator

Mehrfachzuordnung von Team-Rollen

Diese Rollenlogik erlaubt es abweichend von üblichen Modellen, dass ein User durchaus eine Team-Rolle mehrfach zugeordnet werden kann. Er kann ja z.B. Leiter oder auch Mitarbeiter mehrerer Teams sein. Diese Besonderheit erlaubt es erst, die Auflösung der oben beschriebenen Problematik der $m * n$ Dimensionen (m -Rollen und n Projekte), auf die eine Dimension der m -Team-Rollen (siehe **Abbildung 2**).

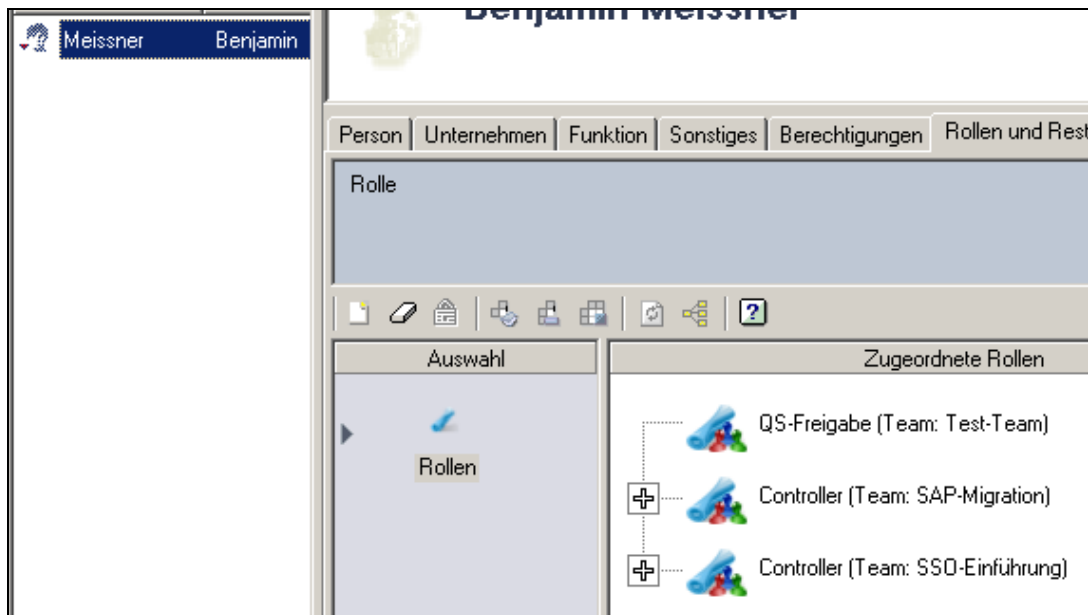


Abbildung 2: Mehrfachzuordnung von gleichen Team-Rollen aber in verschiedenen Projekten

Dynamische Separation of Duties

In Ergänzung des normalen Regelwerks der Festlegung von unzulässigen Rollen-Kombinationen und damit unzulässigen Rechteverbindungen (statische Separation of Duties) ist in dem Rollenmodell für Teams die dynamische Separation of Duties zu berücksichtigen. Diese verhindert unzulässige Rechtekombinationen innerhalb eines Projektes, erlaubt diese aber in verschiedenen Projekten. Beispielsweise kann ein User in einem Team nicht gleichzeitig Leiter und Controller sein. In verschiedenen Projekten ist diese Kombination hingegen durchaus zulässig.

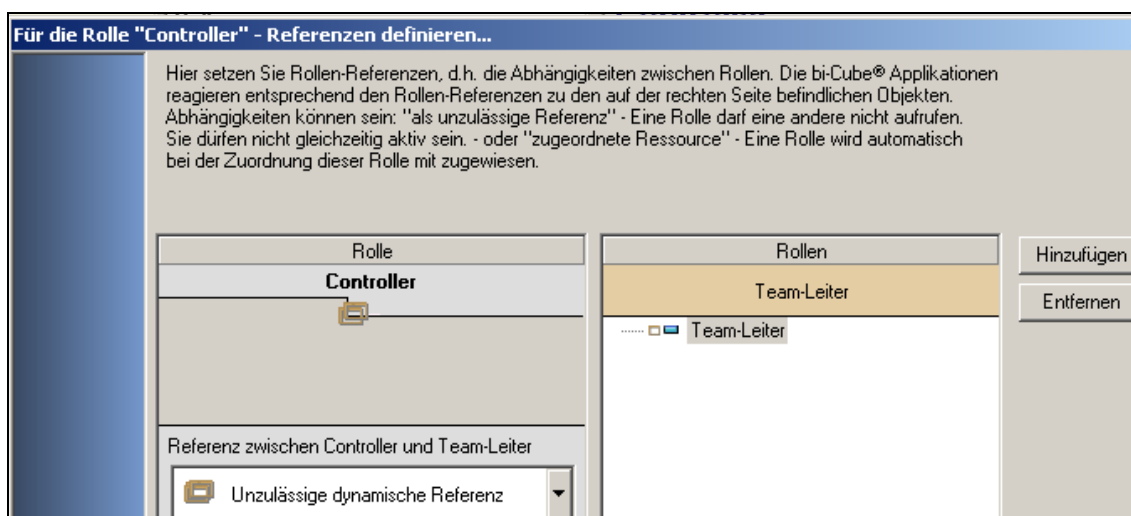


Abbildung 3: Definition einer dynamischen Separation of Duties

2.2 Funktionen in der Teamorganisation

Es wird in diesem Modellansatz davon ausgegangen, dass es Team-übergreifend Projekt-Koordinatoren gibt, die folgende Aufgaben haben:

1. Initialisierung eines neuen Projektes mit den Eckdaten wie Projektdauer bzw. Enddatum, Vertraulichkeitsstufe, evtl. Mandantenbezug, verantwortliche Organisationseinheit
2. Festlegung einiger Schlüsselbegriffe, die den Bezug zu Projektdokumenten und Projektdatenbanken herstellen
3. Zuordnung einer Kostenstelle, auf die die Team-Mitglieder ihren Aufwand buchen können.
4. Berufung von Mitarbeitern in das Team und Benennung eines Team-Leiters.

Die Projektkoordinatoren erhalten im IdM genau diese vordefinierte Rolle mit den Rechten, die es ihnen erlauben, diese Funktionen wahrzunehmen. Sie haben damit den Überblick über alle Projekte und können die Belastung einzelner Mitarbeiter durch die Zuordnung zu mehreren Projekten, die personelle Ausstattung der Projekte mit Kapazitäten untereinander usw. beurteilen. Sie steuern die Dauer von Projekten. Dies ist insbesondere für einen geordneten Abschluss von Projekten zuständig.

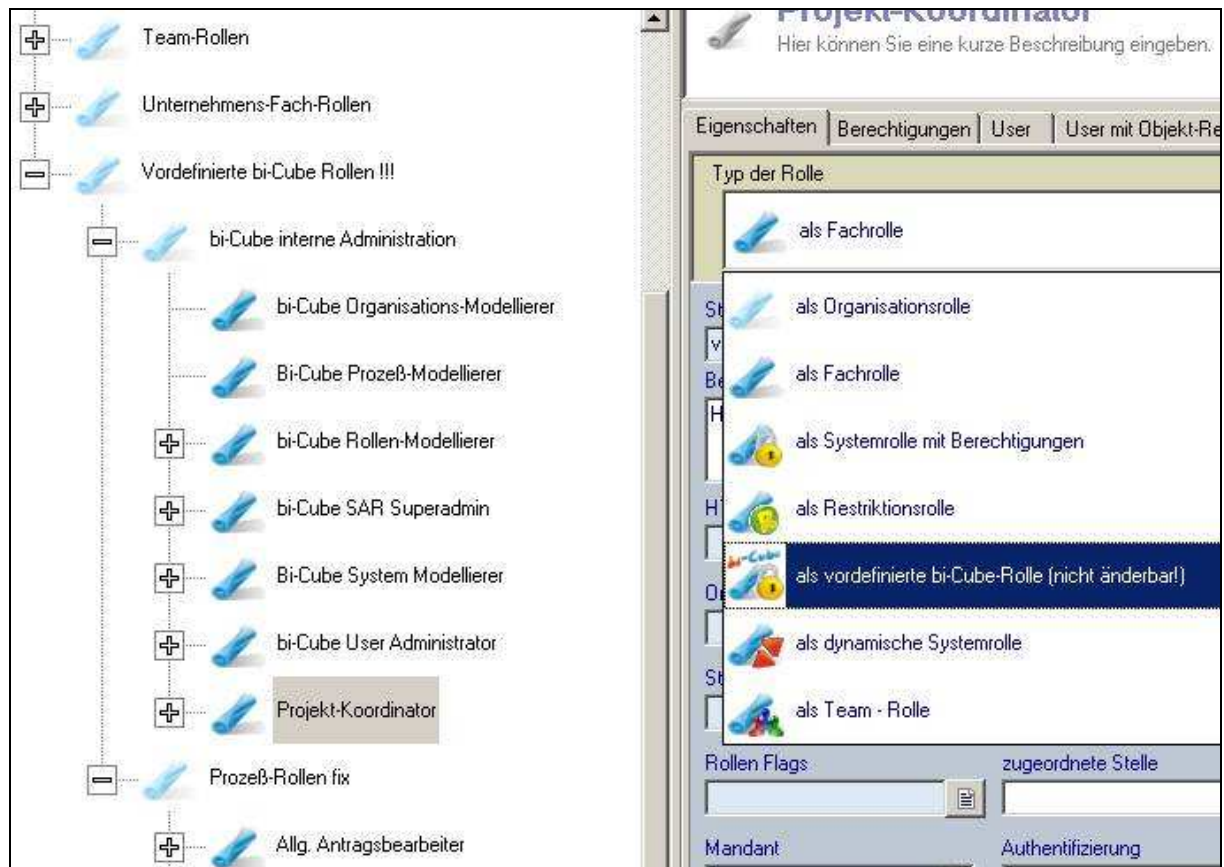


Abbildung 4: Der Projektkoordinator als eine im System vordefinierte Rolle

3 Team-Verwaltung

Die Verwaltung der Mitglieder eines Teams erfolgt über vordefinierte generische Prozesse. In diesen Prozessen wird die Mitgliedschaft eines Users in einem Team organisiert. Es werden je zwei Prozessvarianten für den Ein- und Austritt eines Users in ein Team realisiert:

Direkte Berufung eines Users in ein Team

Der Projektkoordinator kann direkt einen User in ein Team berufen. Dies erfolgt immer direkt im Admin Client und hat immer zwei Informationen zur Folge:

1. Info an den User, dass er Mitglied des Teams und der User XY sein Teamleiter ist
2. Info an den Leiter, dass einer seiner Mitarbeiter in ein Team berufen wurde.

Dieser direkte Zuordnungsprozess enthält nur diese Informationen und keinerlei Genehmigungen, ist also nicht abzulehnen bzw. nicht umkehrbar.

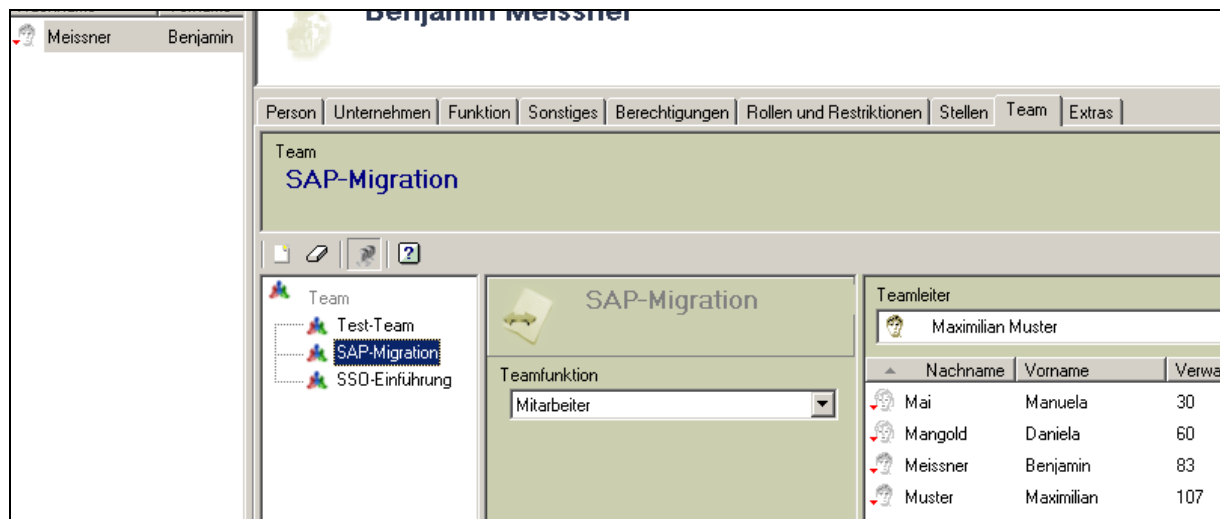


Abbildung 5: Direkte Berufung in ein Team

Antrag auf Team-Mitgliedschaft

Alternativ können im IdM-Web-Portal folgende User als Aktoren fungieren und den Antrag auf Team-Mitgliedschaft eines Users stellen:

- der Projektkoordinator stellt den Antrag an den Leiter eines Users, dieser kann den Antrag ablehnen
- der Leiter stellt den Antrag an den Projektkoordinator, der den Antrag ebenfalls ablehnen kann
- Der Teamleiter stellt den Antrag, der sowohl vom Projektkoordinator als auch vom Leiter (in dieser Reihenfolge) genehmigt werden muss. Wenn der Projektkoordinator ablehnt, ist der Prozess beendet. Ist der Teamleiter gleichzeitig auch Leiter des Users ist, entfällt natürlich dessen Genehmigung.

In jedem Antrag ist anzugeben, für welche Rolle der User vorgesehen ist. Gleichzeitig ist der vorgesehene Zeitraum anzugeben. Alternativ kann der Antrag für die gesamte gestellt werden. Im Antrag muss die prozentuale Belastung des Users durch die Projektarbeit angegeben werden. Ergänzt wird der Antrag durch ein Freitextfeld.

Nach erfolgter Genehmigung wird der User Mitglied des Teams und erhält die beantragte Rolle (evtl. mit einem Enddatum der Rolle) Informationen gehen an alle Beteiligten.

Direkte Abberufung eines Users aus einem Team

Dieser Prozess ist die Umkehrung der direkten Berufung und ist nur durch den Projektkoordinator auszulösen. Er hat die analogen Informationen an den User und dessen Leiter sowie den sofortigen Austritt aus dem Team zu Folge.

Antrag auf Austritt aus dem Team

Dieser Antrag kann im IdM-Web-Portal durch folgende Personen gestellt werden:

1. der User selbst (Freigaben durch 2. und 3.)
2. dessen Leiter (Freigabe durch 3.)
3. der Team-Leiter (Freigabe durch 2.)

Der Antrag enthält die Teamdaten des Users und ein Freitextfeld zur Begründung Informationen gehen an alle Beteiligten

Übersichten im IdM-Web-Portal

Jeder berechtigte User kann sich im IPM-Web-Portal über die laufenden Projekte deren Mitglieder samt Rollen und auch die Projektkosten informieren.

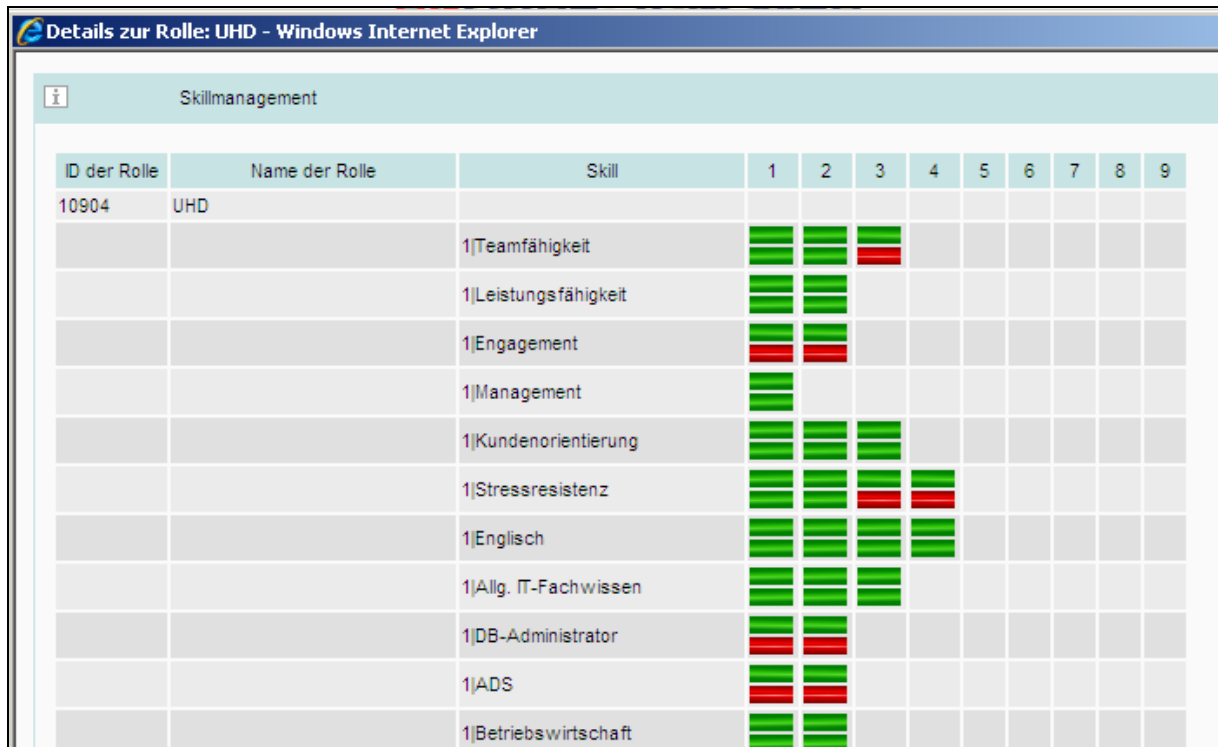


The screenshot displays the 'bi-Cube IPM Web' interface. At the top, there is a navigation bar with tabs for 'Service Center', 'Dokserver', 'SOP-Tools', 'Compliance', and 'Telefonbuch'. Below this, the user's session information is shown: 'Username: y000003' and 'Sitzung endet in: 44:21 min'. The left sidebar contains a 'Service Center' menu with various options like 'Web Kennwort ändern', 'LAN Account Service', 'Objektverwaltung', etc. The main content area is divided into three columns: 'Teamübersicht' (Team Overview) showing a tree structure of teams under 'IT-Projekte', with 'Test-Team' selected; 'Teammitglieder' (Team Members) listing 'Markert, Anton' and 'Meissner, Benjamin'; and 'Team-Rollen des Users' (User Roles) listing roles like 'Controller' and 'QS-Freigabe' for different teams.

Abbildung 6: Allgemeine aber berechtigungsabhängige Informationsplattform zu Projekten

4 Integration des Skill-Managements

Ein leistungsfähiges IdM-System erlaubt es, ein Skill-Management zu integrieren. Dabei wird für die Rollen das Anforderungsmaß an bestimmte Skills definiert. Im Zuordnungsprozess einer Rolle (auch einer Team-Rolle) zu einem User kann der Beantragende und der Genehmiger vor Abschluss seines Task (Antrag oder Freigabe) prüfen, in welchem Maße der User den Anforderungen entspricht, die durch die Rolle gefordert werden.



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	█	█							

Abbildung 7: Vergleich der Anforderungen (grün) einer Rolle und der Erfüllung des Users. Wobei die roten Balken ein entsprechendes Manko deutlich macht.

Mit Hilfe dieser Methodik ist es auch möglich, im ganzen Unternehmen nach geeigneten Team-Mitgliedern zu suchen. Die Skills können beliebig definiert werden. Die im **Abbildung 7** dargestellten Soft-Skills werden durch deutlich quantifizierbare Skills, wie absolvierte Lehrgänge, Zertifikate usw. ergänzt.

Für bestimmte Rollen lassen sich auch „K.O.- Skills“ definieren: Beispielsweise sollte ein Team-Leiter oder ein QS-Manager bestimmte Zertifikate aufweisen, ohne die es nicht möglich ist, eine so bedingte Rolle zu erhalten.