

IPM Web Demo

Inhalt

1	ZIEL	2
2	FUNKTIONSKONZEPT	2
3	TECHNISCHES LÖSUNGSKONZEPT	2
3.1	Systeme	3
3.2	Rollenmodell	4
3.2.1	Attribut-Referenz an Rollen	4
3.2.2	Objekt-Referenz an Rollen	5
3.2.3	Rollenanträge	5
3.2.3.1	Fachrolle Externer Mitarbeiter	5
3.2.3.2	Rolle: Kompetenzen ohne IT-Ressourcen	6
3.2.3.3	Leiter-Rolle	6
3.2.3.4	Rolle Mitarbeiter-Buchhaltung	8
3.2.3.5	Rolle Mitarbeiter Verkäufer	9
3.2.3.6	Rolle Partner	10
3.2.4	Systemantrag	12

IPM Web Demo

1 Ziel

Wir wollen Interessenten potentiellen Kunden und Vertriebspartnern sowie Analysten und Beratern einen Zugang zu unserem IPM Web eröffnen, um bestimmte Funktionen testen zu können.

2 Funktionskonzept

Alle Interessenten bekommen vom iSM Support eine Rolle zugewiesen, die es Ihnen ermöglicht, im Partner Portal für die Organisationseinheit (OE), der sie zugeordnet sind weitere User anzulegen und zu berechtigen. Der Interessent ist für diese OE der Leiter. Er kann keine weiteren Leiter anlegen. Der dann angelegte User dieser OE kann einen Urlaubs- oder Systemantrag stellen oder weitere Rollen beantragen, die der Leiter bestätigen muss.

3 Technisches Lösungskonzept

Basis ist unser produktives Identity & Provisioning Management System, in dem unter einer OE-Rolle einige Demo-Rollen mit den verschiedenen Ausprägungen der Steuerungen angelegt werden. Für diese Demo-Rollen sind Beispielsysteme zu definieren.

Im Einzelnen:

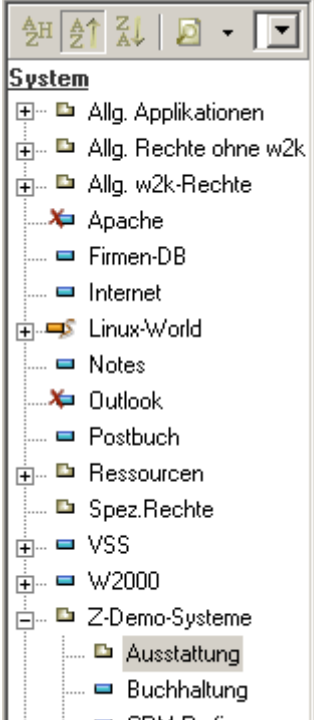
- Demo-System anlegen
- Demo-Rolle 1 mit Demo-System
- Demo-Rolle 2 mit Demo-System
- Anlegen einer Web-Rolle für den Demo-Admin
- Anlegen einer Web-Rolle für den Demo-User

Die Mailadresse ist im Web ein Zwangseingabefeld.

3.1 Systeme

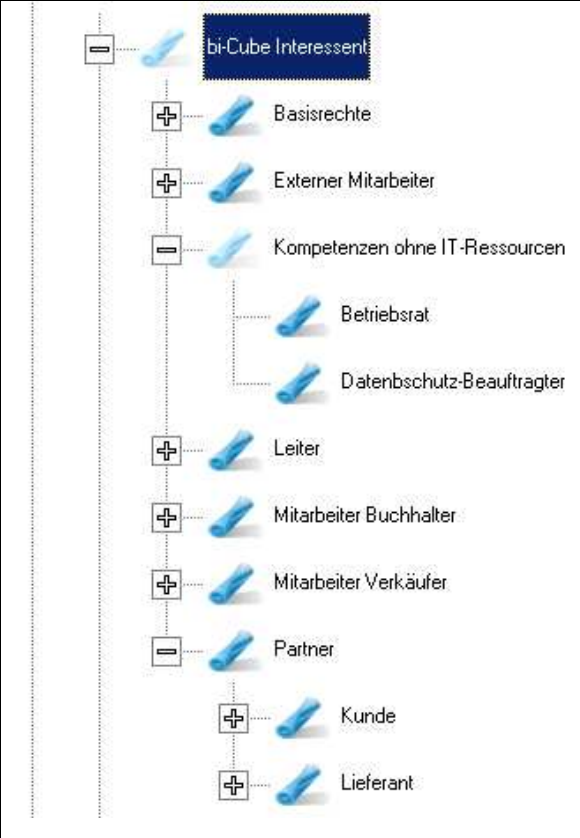
Zur Demonstration der Möglichkeiten wurden drei Systeme angelegt:

- Ausstattung
- Buchhaltung
- CRM-Tool

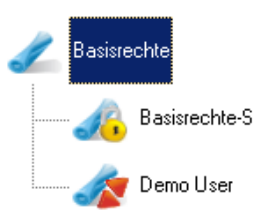
 <p>System</p> <ul style="list-style-type: none"> + Allg. Applikationen + Allg. Rechte ohne w2k + Allg. w2k-Rechte ✗ Apache Firmen-DB Internet + Linux-World Notes ✗ Outlook Postbuch + Ressourcen Spez.Rechte + VSS + W2000 - Z-Demo-Systeme <ul style="list-style-type: none"> Ausstattung Buchhaltung CRM-Profi 	<p>Attribut</p> <ul style="list-style-type: none"> Handy Notebook Signaturkarte Zutrittskarte 	<p>Diese Systeme sind mit unterschiedlichen Eigenschaften versehen:</p> <ul style="list-style-type: none"> - Ausstattung ist als Container definiert, der nur als Hilfsprozess zur nachweisbaren Verwaltung von wertvollen Ausstattungen der Mitarbeiter dient - Das System Buchhaltung ist ein System mit Berechtigungsverwaltung und soll nur in Rollen für Interne Mitarbeiter verfügbar sein. Je Zuteilung fallen 25 Euro in der Internen Kostenverrechnung an. - Das CRM-Tool hat ebenfalls eine interne User- und Berechtigungsverwaltung und dient der Kundenverwaltung. Es kann partiell auch von Zulieferern oder Kunden genutzt werden. Je Zuteilung fallen 12 Euro in der Internen Kostenverrechnung an.
--	--	--

3.2 Rollenmodell

Mit dem Rollenmodell sollen die wesentlichen Funktionen bzw. Nutzungsmöglichkeiten des **bi-Cube®** Rollenmodells praktisch dargestellt werden.

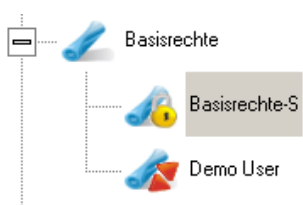
	<p>In der Wurzel ist die Org.-Rolle bi-Cube® Interessent definiert.</p> <p>Darunter befinden sich die Fachrollen (FR): In der Fachrolle Basisrechte sind Rechte definiert, die bestimmte User automatisch beim Eintritt bekommen.</p> <p>Die Bedingung, für welche User das gilt ist in der Attributreferenz festgelegt. Hier wird die Mitarbeitergruppe bi-Cube Demo mit der Fachrolle Basisrechte verbunden.</p> <p>Der Leiter kann seine Mitarbeiter in diese Mitarbeitergruppe einordnen, womit diese dann automatisch die Basisrechte bekommen.</p> <p>Eine weitere Fachrolle definiert Externe Mitarbeiter und deren Rechte, die in der Regel geringer ausfallen als die Rechte fachlich gleichgestellter interner Mitarbeiter.</p>
--	--

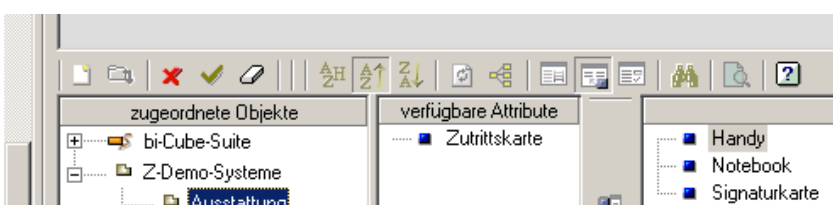
3.2.1 Attribut-Referenz an Rollen



Stammattribut	Operator	Wert	Inhalt
Mitarbeitergruppe	OR	7	bi-Cube Demo

Wie oben definiert, erhält damit ein externer Mitarbeiter (so wie auch die beiden Mitarbeiter Buchhaltung und Verkauf) aus der Menge an möglichen Ausstattungen eine Zutrittskarte.





3.2.2 Objekt-Referenz an Rollen

<p>Rolle</p> <p>Basisrechte</p> <p>Referenz zwischen Basisrechte und Leiter</p> <p>zugeordnete Ressource</p> <p>Hinweis: Die oben auf der linken Seite angegebene Rolle wird automatisch mit zugewiesen.</p>	<p>Leiter</p>	<p>Damit der Leiter selbst diese Basisrechte auch bekommt, wird die Rolle Leiter als Objekt-Referenz mit der Rolle Basisrechte verbunden.</p>
--	---------------	---

In der Übersicht stellt es sich dann so dar:

Dass die Rolle referenziert und nicht direkt zugeordnet ist, ist an dem kleinen Dreieck in der Graphik ersichtlich.

3.2.3 Rollenanträge

3.2.3.1 Fachrolle Externer Mitarbeiter

Der Externe erhält in diesem Beispiel ein Notebook ausgehändigt aber keinerlei Rechte an den beiden IT-Systemen (CRM und Buchhaltung)

Eigenschaften der Rolle:

Die Rolle ist mit dem Userattribut Mitarbeitergruppe Gruppe 2 (= Externer Mitarbeiter) indiziert:

IPM Web Demo

Attributindizierung (Satznummer) zu:			
Externer Mitarbeiter			
Stammattribut	Oper...	Wert	
Mitarbeitergru...	OR	2	

Dadurch wird festgelegt, dass diese Rolle nur Externe bekommen können. Nach welcher Regel dies dann abgewickelt wird, macht die Einstellung in der Flagliste deutlich:

FLAGLISTE	
Flagliste	
1. Flag	
<input checked="" type="radio"/>	Rolle ist genehmigungspflichtig
<input type="radio"/>	Rolle ist nicht genehmigungspflichtig
2. Flag	
<input type="radio"/>	Rolle kann vom Leiter und vom User beantragt werden
<input type="radio"/>	Rolle kann nur vom Leiter beantragt werden (Fremdantrag)
<input checked="" type="radio"/>	Rolle kann nur vom User beantragt werden (Eigenantrag)
<input type="radio"/>	Rolle kann automatisch beantragt werden

Dies bedeutet, dass diese Rolle durch den User beantragt werden kann und vom Leiter zu bestätigen ist.

3.2.3.2 Rolle: Kompetenzen ohne IT-Ressourcen

Diese Rolle dokumentiert die Möglichkeit, FR zu definieren, unter denen keine Systemrollen (SR) mit dedizierten Rechten auf IT-Systemen angeordnet sind.

Diese Möglichkeit kann genutzt werden, um diese Kompetenz in einer beliebigen Weise an andere Systeme weiterzureichen oder diese Rolle in der internen Prozesssteuerung zu nutzen. Beispielsweise kann bei der Vergabe einer Rolle mit einer hohen Security Classification im Antragsverfahren der Beauftragte für Datenschutz eine Info bekommen oder auch diese Rolle noch zusätzlich freigeben.

3.2.3.3 Leiter-Rolle

Diese Rolle bekommt der Mitarbeiter des Unternehmens, der vom iSM berechtigt wird, für sein Unternehmen einige Demo-Funktionen zu nutzen. Gleichzeitig bekommt er durch den Eintrag der OE-Kompetenz **Leiter** die Sicht auf alle User seiner OE zugeteilt. (Bzw. die entsprechende Einschränkung)

IPM Web Demo



The screenshot shows a role configuration window titled "FLAGLISTE" with the subtitle "Flagliste". It contains three sections of flags:

- 1. Flag**
 - Rolle ist genehmigungspflichtig
 - Rolle ist nicht genehmigungspflichtig
- 2. Flag**
 - Rolle kann vom Leiter und vom User beantra
 - Rolle kann nur vom Leiter beantragt werden
 - Rolle kann nur vom User beantragt werden (
 - Rolle kann automatisch beantragt werden
- 3. Flag**
 - Schnittstelle DB_OUT (DBOC) ist inaktiv, d.h.
 - Schnittstelle DB_OUT (DBOC) ist aktiv, d.h. .
 - Schnittstelle DBOUT (eOrgDB OC) ist aktiv

To the left, a list of roles is shown with expand/collapse icons:

- Z-Demo
- Demo Testleiter
- Demo Fachtester
- Demo Secu-Token
- Demo Richtlinien
- bi-Cube Interessent
- Leiter

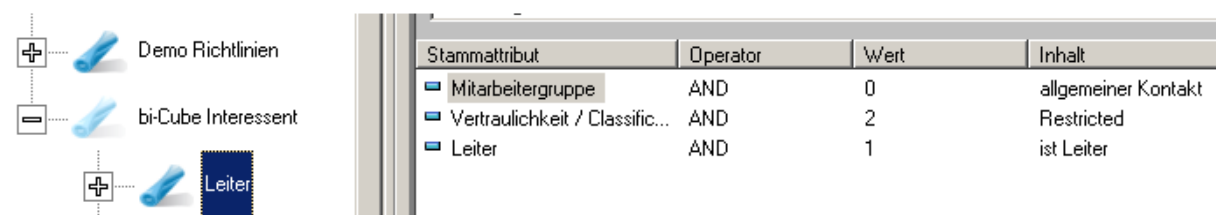
Diese Rolle wird mit User-Attributen indiziert:

Am User selbst sind folgende Einstellungen vorzunehmen:

1. in der Mitarbeitergruppe muss stehen: **allgemeiner Kontakt**
2. Ist im iSM die SC auf **Restricted** zu setzen
3. im Feld M_Gruppe ist auszuwählen: **ist Leiter**

Daraus wird die Regel abgeleitet, dass ein externer Partner mit diesen drei Eintragungen die Rolle **Leiter** zugeordnet bekommt.

Damit der entsprechende User seine Zuordnungsdaten bekommt, ist darauf zu achten, dass er eine gültige Mailadresse hat (kein Info@... oder ähnliches).



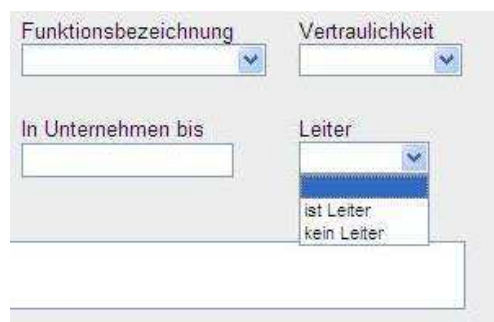
The screenshot shows the role configuration interface with a table of attributes:

Stammattribut	Operator	Wert	Inhalt
Mitarbeitergruppe	AND	0	allgemeiner Kontakt
Vertraulichkeit / Classific...	AND	2	Restricted
Leiter	AND	1	ist Leiter

To the left, the role list is updated to show "Leiter" as selected.

Damit sollte der **Leiter** diese Rolle bekommen.

Im Web sind dazu die entsprechenden Einstellungen vom iSM vorzunehmen:



The screenshot shows the iSM web interface with the following fields:

- Funktionsbezeichnung: [Dropdown menu]
- Vertraulichkeit: [Dropdown menu]
- In Unternehmen bis: [Text input field]
- Leiter: [Dropdown menu with options: "Leiter", "ist Leiter", "kein Leiter"]

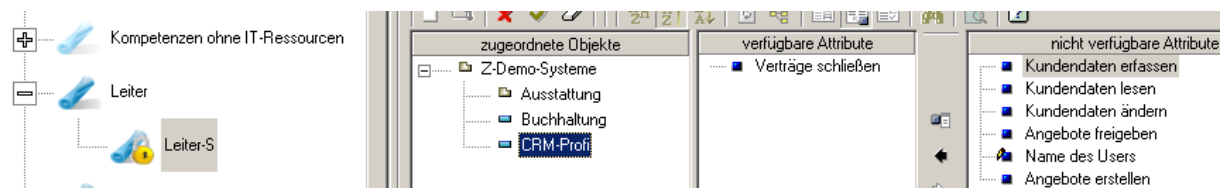
IPM Web Demo

Rechte des Leiters

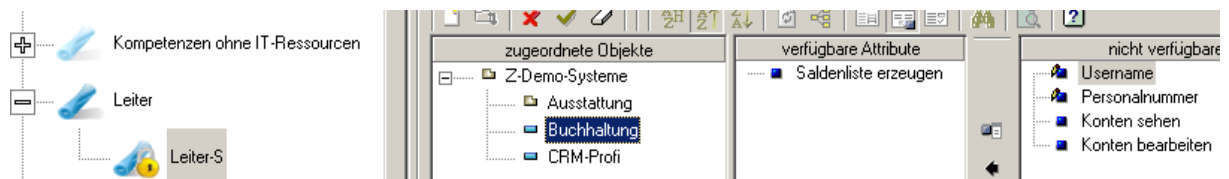
Der Leiter erhält innerhalb seiner Rolle folgende Rechte:



Er bekommt das Nutzungsrecht an einem Diensthandy und erhält eine Signaturkarte, um im iSM-System mit Hilfe der digitalen Signatur einen Vertrag final abzuschließen.



Außerdem kann er innerhalb der Buchhaltung Saldenlisten erzeugen



3.2.3.4 Rolle Mitarbeiter-Buchhaltung

FLAGLISTE Flagliste	Diese Rolle ist genehmigungspflichtig und kann vom Mitarbeiter oder Leiter beantragt werden.
<p>1. Flag</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> Rolle ist genehmigungspflichtig <input type="radio"/> Rolle ist nicht genehmigungspflichtig <p>2. Flag</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> Rolle kann vom Leiter und vom User beantragt werden <input type="radio"/> Rolle kann nur vom Leiter beantragt werden (Fremdantrag) <input type="radio"/> Rolle kann nur vom User beantragt werden (Eigenantrag) <input type="radio"/> Rolle kann automatisch beantragt werden 	

IPM Web Demo

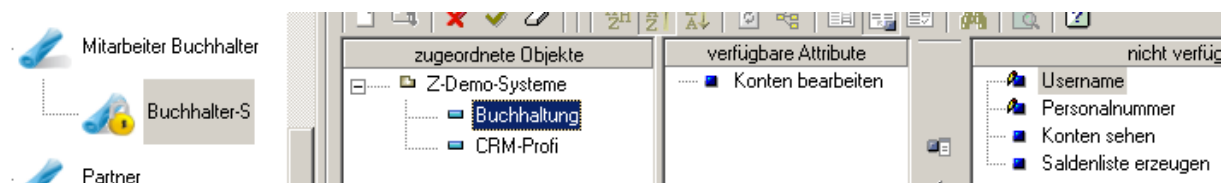
Attributindizierung (Satznumr		
Mitarbeiter Buchhalter		
Stammattribute	Oper...	Wert
■ Mitarbeitergru...	OR	2

Vergleichswert
 NOT

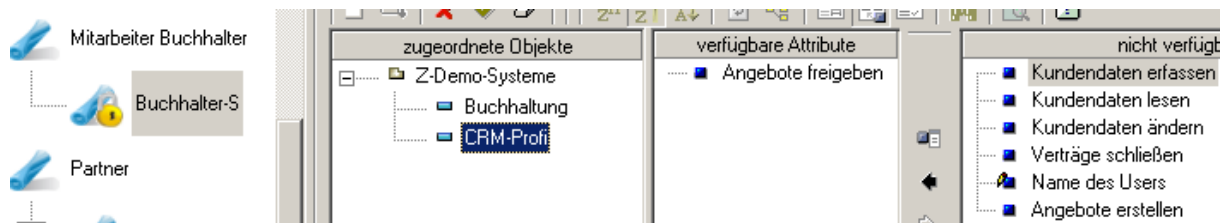
Verknüpfung

Über die Mitarbeitergruppe ist sie jedoch so indiziert worden, dass sie ein Externer nicht erhalten kann.

Sie hat folgende Rechte:
 Es können natürlich Konten bearbeitet werden

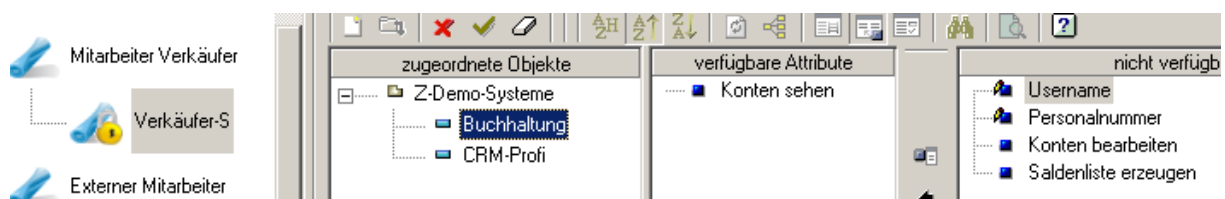


und das iSM-System ist so konfiguriert, dass die Buchhaltung Angebote final freigeben muss (z.B. nach Prüfung des Zahlungsverhaltens des Kunden)



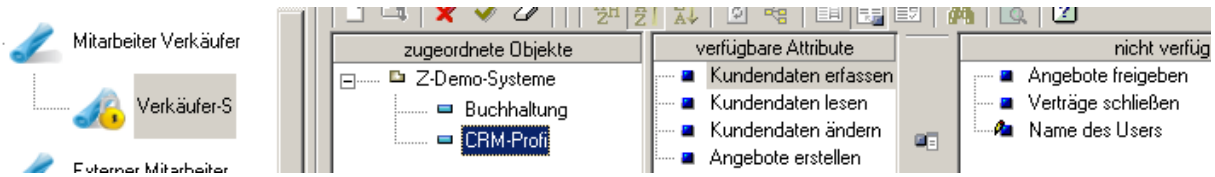
3.2.3.5 Rolle Mitarbeiter Verkäufer

Analog ist die Rolle des Verkäufers definiert.
 In der Buchhaltung kann er potentielle Kunden z.B. auf den bisherigen Umsatz prüfen und dann



im iSM-System entsprechend agieren.

IPM Web Demo



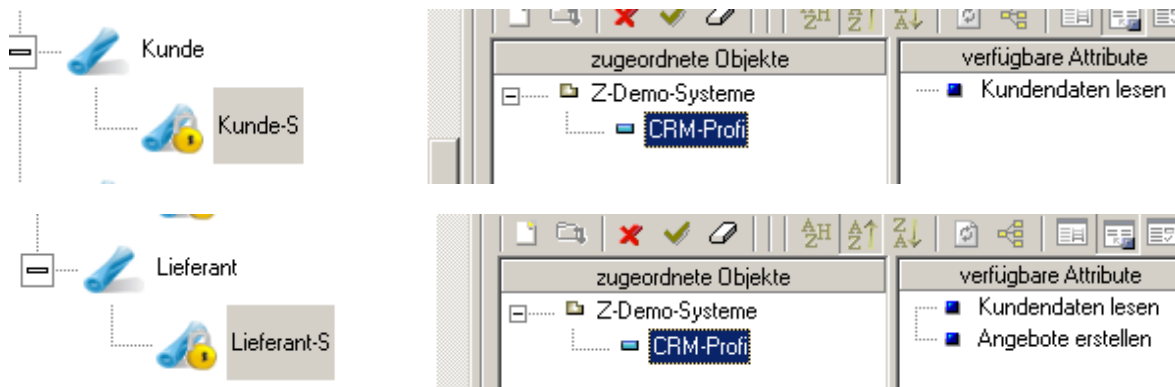
Die Einschränkung der Beantragung und Genehmigung ist analog der Buchhaltung.

3.2.3.6 Rolle Partner

Diese Fachrolle demonstriert die Möglichkeit, Fachrollen hierarchisch zu modellieren und damit auch die Vererbung der Rechte zu erreichen.

	<p>Ein User ist gleichzeitig Kunde und Lieferant: Wenn ihm dann die FR Partner zugeordnet wird erhält er sowohl die FR Kunde als auch die FR Lieferant und damit die beiden FR zugeordneten Rechte in ihrer Vereinigung.</p> <p>Selbstverständlich können die beiden FR (Kunde, Lieferant) einem User auch separat zugeordnet werden.</p>
--	---

Die Rechte sind wie dargestellt, definiert:

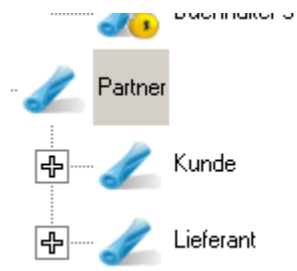


Wichtig ist bei dieser hierarchischen Anordnung von Fachrollen, dass die Vererbung berücksichtigt wird. D.h. Die Rolle **Partner** enthält sowohl die Rechte **Kunde** als auch die Rechte **Lieferant**.

Die Vererbung kombiniert dann natürlich auch die Rollen-Regeln in Richtung Genehmigungspflicht usw. Aus dieser Sicht muss hier eine sinnvolle Modellierung der Regeln beachtet werden.

Es macht z.B. nicht recht Sinn, wenn die Einzelrollen (Kunde und Lieferant) genehmigungspflichtig sind und die zusammenfassende Rolle ebenfalls. Diese sollte dann nicht mehr genehmigungspflichtig sein.

IPM Web Demo



Flagliste

- Flag**
 - Rolle ist genehmigungspflichtig
 - Rolle ist nicht genehmigungspflichtig
- Flag**
 - Rolle kann vom Leiter und vom User beantragt werden
 - Rolle kann nur vom Leiter beantragt werden (Fremdantrag)

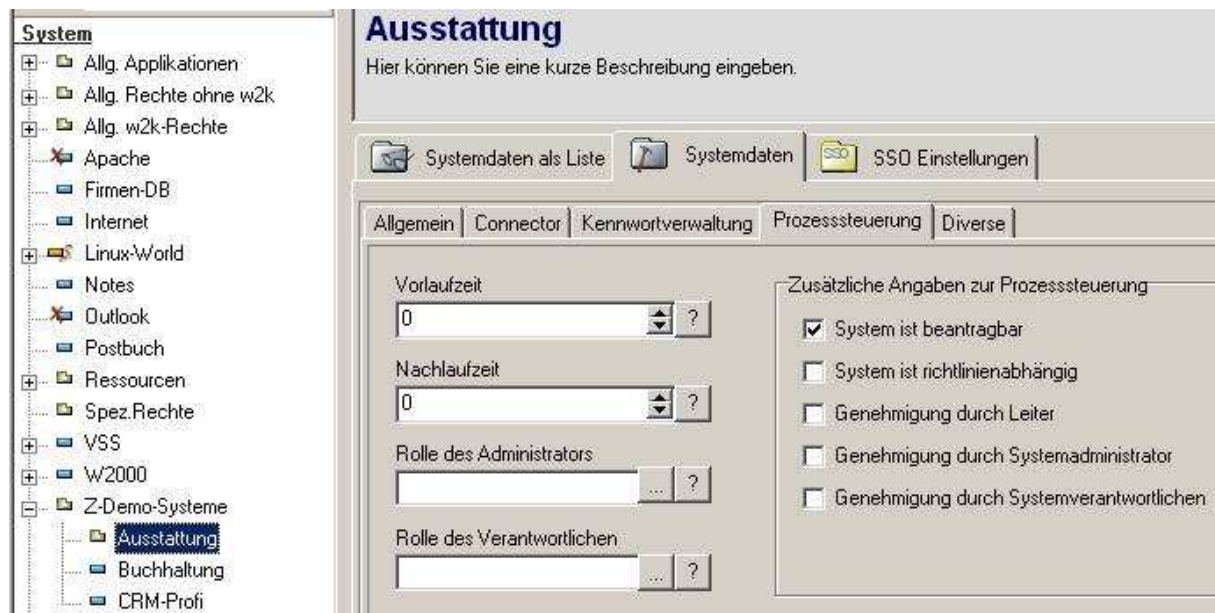
3.2.4 Systemantrag

Um auch einen Systemantrag stellen zu können, muss im Object Manager die Einstellung in den Sytemdaten entsprechend konfiguriert werden.

Das System Ausstattung wird deshalb mit dem Flag **System ist beantragbar** versehen. muss.

Richtlinienabhängig kann das System definiert werden, wenn der User eine Richtlinie bestätigen muss, bevor ihm das System zugeordnet wird.

Je nach Notwendigkeit können im Genehmigungs-Prozess weitere Genehmigungen eingefügt werden.



System

- Allg. Applikationen
- Allg. Rechte ohne w2k
- Allg. w2k-Rechte
- Apache
- Firmen-DB
- Internet
- Linux-World
- Notes
- Outlook
- Postbuch
- Ressourcen
- Spez.Rechte
- VSS
- W2000
- Z-Demo-Systeme
 - Ausstattung**
 - Buchhaltung
 - CRM-Profi

Ausstattung

Hier können Sie eine kurze Beschreibung eingeben.

Systemdaten als Liste | Systemdaten | SSO Einstellungen

Allgemein | Connector | Kennwortverwaltung | **Prozesssteuerung** | Diverse

Vorlaufzeit: 0

Nachlaufzeit: 0

Rolle des Administrators: ... ?

Rolle des Verantwortlichen: ... ?

Zusätzliche Angaben zur Prozesssteuerung

- System ist beantragbar
- System ist richtlinienabhängig
- Genehmigung durch Leiter
- Genehmigung durch Systemadministrator
- Genehmigung durch Systemverantwortlichen