Antrag auf Zuteilung einer Rolle

1 Ziel

Beim Rollenantrag werden folgende Funktionen realisiert:

1. Im Antragsverfahren (bi-Cube Web-Portal) kann ein User für sich selbst (Eigenantrag) oder eine berechtigte Person (z.B. der Leiter) für andere (Fremdantrag) Anträge auf Zuteilung einer neuen Rolle stellen. Dabei sorgt die Attributindizierung der Fachrollen dafür, das jeder User nur die Rollen beantragen kann, die für ihn vorgesehen sind bzw. jeder Leiter nur die Rollen aus einem Pool beantragen kann, die für alle seine Mitarbeiter vorgesehen sind.
2. Sollte es im Mitarbeitereintritt zu Fehlern bei der automatischen Zuteilung von (Basis-) Rollen gekommen sein (diese wurden nicht zugeordnet), können die Rollen im Nachgang manuell beantragt werden.
3. Wenn in einer Rolle ein genehmigungspflichtiges System abgelehnt wird, dann werden die Rolle und damit alle zur Rolle gehörenden Systeme nicht zugeordnet.
4. Der User bestätigt vor der Zuweisung richtlinienabhängige Systeme in der Rolle. Lehnt er eine Richtlinie ab, dann werden die betroffene Rolle und damit alle zur Rolle gehörenden Systeme nicht zugeordnet.

Um den Rollenantrag als einen Prozess zu betrachten, werden alle beantragten Rollen intern verwaltet und die Zuordnungen werden komplett kontrolliert. Der Rollenantrag ist erst dann abgeschlossen, wenn alle beantragten Rollen zugeordnet sind. Aus dieser Liste fallen die nicht genehmigten Rollen heraus.

Zum Ende des Prozesses erhält der Antragsteller eine Aufstellung per Email:

- Rolle xy zugeordnet – Timestamp
- Rolle ab durch <Leiter> abgelehnt – Timestamp
- Rolle…

Weiterhin in der Info-Mail enthalten sind die Anmeldenamen (Accounts) für neu zugeordnete Systeme sowie die Erstanmeldepasswörter.

2 Modellierungsrichtlinien

Die Modellierung im Rollenmodell sollte so erfolgen, dass die sog. Zugangssysteme (LAN, Host) und das Mailsystem ohne Freigabe zugeordnet werden können und im manuellen Rollenantrag und damit in diesem GPM nicht betroffen sind. Sie sollten in einer so genannten Basisrolle enthalten sein, die unabhängig von anderen Rollen zugeordnet wird. Damit wird gesichert, dass zusätzliche Berechtigungen (z.B. Filespace im AD) in einer Systemrolle unter einer Fachrolle bereits einen entsprechenden Account vorfinden.

Systeme, die sogenannte technische Attribute beinhalten, die erst bei Antragstellung mit Werten befüllt werden können, sind als Zwang zu vereinbaren. Benötigt das System zusätzliche Userinformationen (Werte aus Userattributen), die für die Verwaltung der Userdaten nicht als Zwang definiert sind, sind diese Userattribute auf entsprechende Systemattribute zu referenzieren und die Systemattribute als Zwang zu vereinbaren. Damit wird bei Antragstellung letztendlich die Befüllung dieser Userattribute durch den Antragsteller sichergestellt.

Soll im Unternehmen ein gewisser Pool von Rollen uneingeschränkt für alle Teilnehmer am Antragsverfahren verfügbar sein (z.B. nicht lizenzpflichtige Grafik-Tools), dann werden diese Rollen im Rollenmodell unter einem Rollencontainer (Organisationsrolle) abgelegt. Diese Organisationsrolle wird im Customizing zum Antragverfahren als Container *Allgemein verfügbare Rollen* eingestellt und so kann sich jeder Teilnehmer aus diesem Pool bedienen.

3 GPM Rolle zuteilen

Der Antrag auf Zuteilung einer neuen Rolle wird im bi-Cube Web-Portal gestellt.

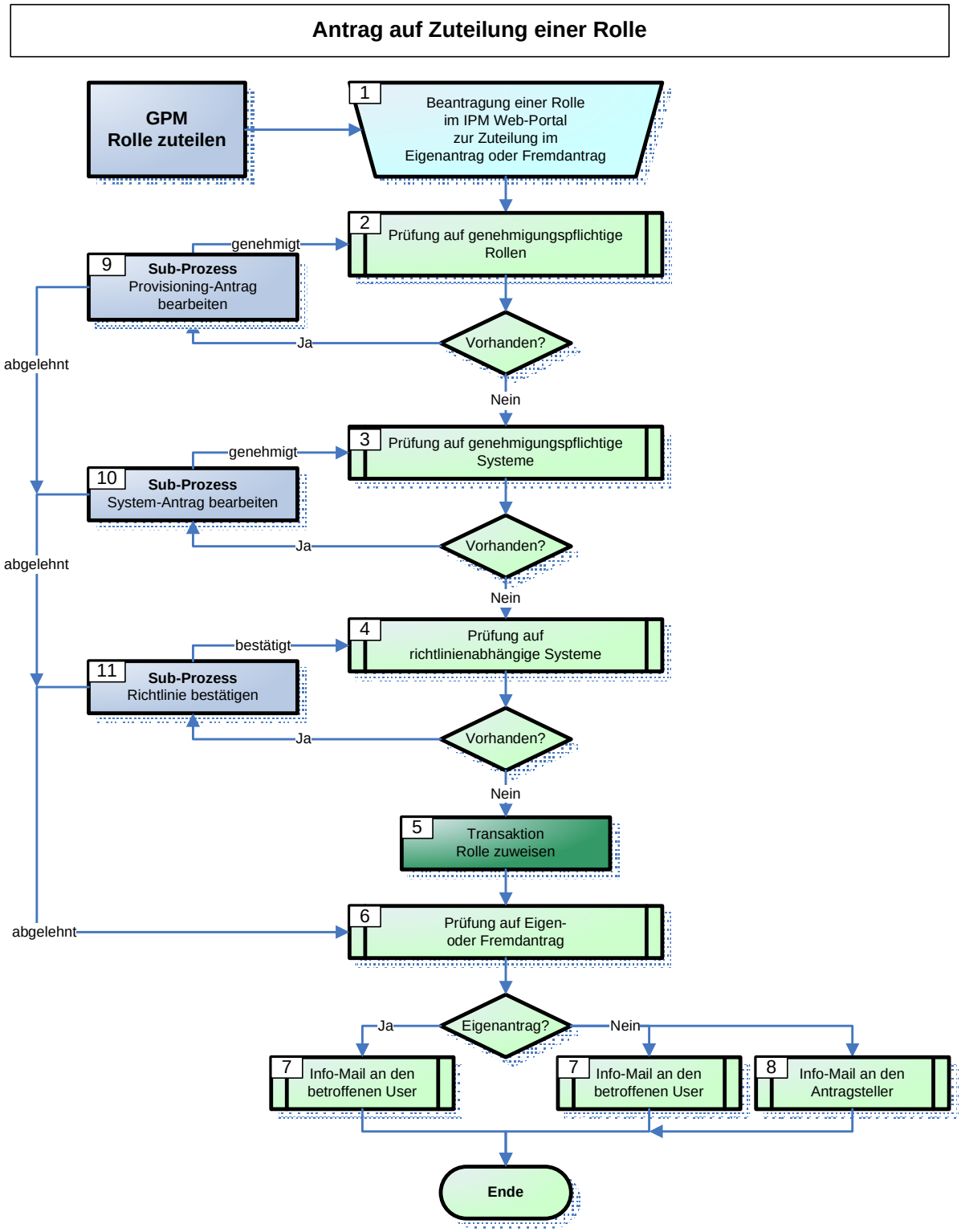

Abbildung 1: GPM Rolle zuteilen

Erläuterungen zum GPM *Rolle zuteilen*

1 **Rollenantrag im Web-Portal stellen:**
Der Antrag kann durch den User selbst oder eine berechtigte Person (z.B. den Leiter) für den betroffenen User gestellt werden. Die Prüfung und Befüllung der Userattribute und der technischen Attribute werden bei Antragstellung durchgeführt. Dabei sind die zu befüllenden Userattribute an dieser Stelle Systemzwangsattribute, die auf Userattribute referenziert sind und damit bei Antragstellung durch den Antragsteller ausgefüllt werden müssen.

2 **Prüfung auf genehmigungspflichtige Rollen:**
Ja: Bei positivem Prüfergebnis wird in den Subprozess *Provisioning-Antrag bearbeiten* verzweigt (siehe Punkt 9)
Nein: Sind keine genehmigungspflichtigen Rollen im Antrag vorhanden bzw. ist die Genehmigung erteilt, wird intern zur nächsten Aktion weitergeleitet (siehe Punkt 3).

3 **Prüfung auf genehmigungspflichtige Systeme:**
Ja: Bei positivem Prüfergebnis wird in den Subprozess *Systemantrag bearbeiten* verzweigt (siehe Punkt 10)
Nein: Sind keine genehmigungspflichtigen Systeme vorhanden bzw. die Genehmigungen erteilt, wird intern zur nächsten Aktion weitergeleitet (siehe Punkt 4).

4 **Prüfung auf richtlinienabhängige Systeme:**
Diese Prüfung findet auf Systemebene statt. Werden richtlinienabhängige Systeme gefunden, wird der betroffene User aufgefordert, die Richtlinie nachweislich zur Kenntnis zu nehmen.
Ja: Bei positivem Prüfergebnis wird in den Subprozess *Richtlinie bestätigen* verzweigt (siehe Punkt 11)
Nein: Sind keine richtlinienabhängigen Systeme vorhanden bzw. alle erforderlichen Richtlinien bestätigt, wird intern zur nächsten Aktion weitergeleitet (siehe Punkt 5).

5 **Transaktion Rolle zuweisen (siehe auch Beschreibung der Transaktionen):**
Die Berechtigungen werden automatisch zugewiesen. Der Logon-Name für die Subsysteme wird über eine Bildungsregel pro Subsystem automatisch vergeben und wenn erforderlich ein Passwort generiert. Die Zuweisungen (Transaktionen) werden vom Transaktionsmonitor überwacht und Fehlermeldungen aus den Schnittstellen (Connectoren) an die bi-Cube Administration gemeldet. Nach erfolgreichem Abschluss aller Transaktionen wird intern zur nächsten Aktion weitergeleitet (siehe Punkt 6).

6 **Prüfung auf Eigen- oder Fremdantrag:**
Durch diese Prüfung soll die Verteilung Abschluss-Mail gesteuert werden. Dabei wird ermittelt, ob der User für sich selbst einen Antrag gestellt hat (Eigenantrag) oder ob eine berechtigte Person für andere einen Antrag gestellt hat (Fremdantrag).
Eigenantrag: Die Abschluss-Information wird nur an den User verschickt (siehe Punkt 7).
Fremdantrag: Die Abschluss-Mail wird an den User und zusätzlich an den Antragsteller verschickt (siehe Punkt 8).

7 **Info-Mail an den betroffenen User:**
Sind alle Berechtigungen zugewiesen, wird der User über den Abschluss des Rollenantrags informiert. Er erhält die Zugangsdaten (Accounts mit Passwörtern für Erstanmeldung) neu vergebener Systemzugänge per Email.

8 **Info-Mail an den Antragsteller:**
Sind alle Berechtigungen zugewiesen, wird der Antragsteller zusätzlich zum User über den Abschluss des Rollenantrags informiert, wenn Antragsteller nicht gleich betroffener User (Fremdantrag). Er erhält per Email die Informationen über zugeteilte Rollen.

9 **Sub-Prozess Provisioning-Antrag bearbeiten (siehe auch Beschreibung der Sub-Prozesse):**
Sind genehmigungspflichtige Rollen für den betroffenen Mitarbeiter zur Zuweisung vorgesehen, wird in diesem Subprozess die Freigabe der Rollen vom zuständigen Leiter eingeholt. Lehnt der Leiter eine Rolle ab, wird diese nicht zugewiesen. Im Sub-Prozess werden definierte Bearbeitungszeiträume überwacht und ggf. Vertreter benachrichtigt bzw. Timeout-Informationen verschickt.'
Sind alle genehmigungspflichtigen Rollen freigegeben, leitet der Prozess-Manager intern zur nächsten Aktion lt. Modell weiter.

10 **Sub-Prozess Systemantrag bearbeiten (siehe auch Beschreibung der Sub-Prozesse):**
Sind lt. der freigegebenen Rollen genehmigungspflichtige Systeme für den betroffenen Mitarbeiter zur Zuweisung vorgesehen, wird in diesem Subprozess die Freigabe der Systeme vom jeweiligen System-Owner (auch Applikationsverantwortlichen) und / oder vom System-Admin (technisch Verantwortlichen) eingeholt. Lehnt ein Genehmiger ab, dann werden die übergeordnete Fachrolle und damit alle zu dieser Rolle gehörenden Systeme nicht zugeordnet.
Im Sub-Prozess werden definierte Bearbeitungszeiträume überwacht und ggf. Vertreter benachrichtigt bzw. Timeout-Informationen verschickt.
Sind alle genehmigungspflichtigen Systeme freigegeben, leitet der Prozess-Manager intern zur nächsten Aktion lt. Modell weiter.

11 **Subprozess Richtlinie bestätigen (siehe auch Beschreibung der Sub-Prozesse):**
Sind richtlinienabhängige Systeme in der Rolle vorhanden, wird der User per Email aufgefordert, die Richtlinie zu lesen und die Kenntnisnahme zu bestätigen. Lehnt er die Richtlinie ab bzw. bestätigt er nicht innerhalb eines vorgegebenen Zeitraums, dann werden die betroffene Rolle und damit alle zur Rolle gehörenden Systeme nicht zugeordnet.