Volker Lehnert, Katharina Stelzner, Peter John, Anna Otto

SAP-Berechtigungswesen

2. Auflage, 978-3-8362-1825-2

Bonuskapitel aus der 1. Auflage (978-3-8362-1349-3):

- »Technische Grundlagen der Berechtigungspflege«
- »Automatisierte organisatorische Differenzierung: der Rollenmanager«

Galileo Press

Bonn • Boston

In diesem Kapitel erfahren Sie, wie Sie Benutzer und Rollen anlegen können. Darüber hinaus soll ein grundlegendes Verständnis der Wirkung von Berechtigungen geschaffen werden.

6 Technische Grundlagen der Berechtigungspflege

Das technische Berechtigungskonzept von SAP ERP ist ein positives Berechtigungskonzept: Das heißt, Sie müssen ausdrücklich festlegen, was ein Benutzer darf. Eine Ausnahme von diesem Prinzip gibt es in SAP ERP HCM, dort gibt es den Ausschluss der eigenen Personalnummer (siehe Kapitel 14, »Berechtigungen in SAP ERP HCM«).

Die Berechtigungen in SAP ERP werden überwiegend über Rollen verwaltet (SAP ERP HCM bietet noch weitere Möglichkeiten, siehe ebenfalls Kapitel 14), die einem Benutzer zugewiesen werden. Eine Rolle besteht aus Transaktionen und Berechtigungsobjekten. Die Berechtigungsobjekte sind im Berechtigungsprofil zusammengefasst und enthalten Berechtigungsfelder, in denen Aktivitäten und weitere Werte, wie z. B. Organisationsebenen, ausgeprägt werden.

In diesem Kapitel werden die zentralen Begriffe und Konzepte der Berechtigungspflege nacheinander vorgestellt. Zunächst beschreiben wir in Abschnitt 6.1, »Benutzer/Berechtigung«, wie ein Benutzer erstellt wird. In Abschnitt 6.2, »Transaktion – Programm – Berechtigungsobjekt«, werden Transaktionen, Programme und Berechtigungsobjekte vorgestellt. Im Anschluss daran lernen Sie Rollen und Rollenprofile in Abschnitt 6.3, »Rollen und Rollenprofile«, kennen. In den beiden letzten Abschnitten dieses Kapitels behandeln wir die Analyse von Berechtigungsprüfungen (Abschnitt 6.4, »Analyse von Berechtigungsprüfungen«) sowie weitere Rollentypen in SAP ERP (Abschnitt 6.5, »Weitere Rollentypen in SAP ERP«).

6.1 Benutzer/Berechtigung

Benutzerpuffer

Damit eine Person im SAP-System eine Aktion ausführen kann, benötigt sie zunächst einen Benutzer(-stammsatz), dem die notwendigen Berechtigungen zugeordnet sind. Zu diesem Zweck werden dem Benutzer Rollen zugeordnet, zu denen jeweils Berechtigungsprofile gehören, die die tatsächlichen Berechtigungen enthalten. Bei der Anmeldung eines Benutzers am System werden alle Berechtigungen, die ihm zugeordnet sind, in den *Benutzerpuffer* geladen. Sämtliche Berechtigungsverprobungen finden gegen den Benutzerpuffer statt.

Abbildung 6.1 zeigt einen Benutzer, dem eine Rolle zugeordnet ist, die Rolle enthält Transaktionen, ein Menü und ein Profil, das aus Berechtigungsobjekten besteht.

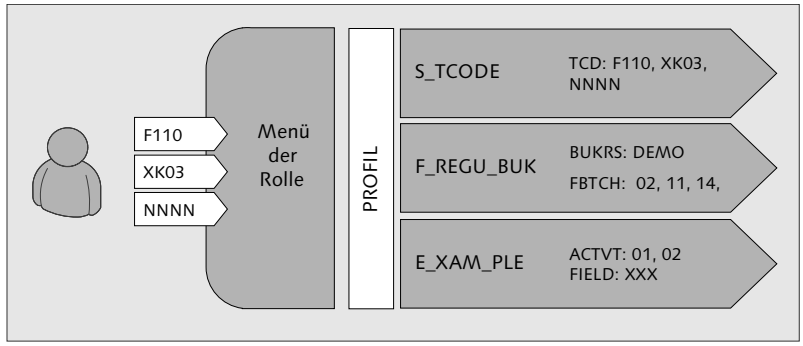


Abbildung 6.1 Benutzer und Berechtigungen

Die verschiedenen Benutzertypen sowie die Benutzerpflege werden im Folgenden genauer beschrieben.

6.1.1 Benutzer

Unterschiedliche Benutzertypen

Alle Aktionen im SAP-System werden durch Benutzer ausgeführt. Dabei gibt es unterschiedliche Benutzertypen für unterschiedliche Arten von Aktionen.

- Dialogbenutzer
- Servicebenutzer
- Kommunikationsbenutzer
- Systembenutzer
- Referenzbenutzer

Dialogbenutzer

Dialogbenutzer sind für natürliche Personen personalisierte Benutzer, die sich über das SAP GUI am System anmelden. Der Dialogbenutzer ist der zentrale Benutzertyp, er steht deshalb in diesem Buch im Vordergrund.

Servicebenutzer

Servicebenutzer dienen z. B. in Webservices dem anonymen Zugriff mehrerer Benutzer. Aus diesem Grund sollten die Berechtigungen für diesen Benutzertyp stark eingeschränkt werden. Das bedeutet auch, dass nur ein Benutzeradministrator das Kennwort ändern kann. Die Anwender melden sich über das SAP GUI an, dabei ist es möglich, dass sie sich mehrfach anmelden. Es wird nicht vom System überprüft, ob das Kennwort abgelaufen oder initial ist.

Kommunikationsbenutzer

Kommunikationsbenutzer sind systematisch personenbezogene Benutzer, die sich allerdings nicht über das SAP GUI, sondern über RFC-Aufruf (*Remote Function Call*) anmelden. In diesem Fall ist es dem Benutzer möglich, das Kennwort zu ändern. Es erfolgt eine Prüfung, ob das Kennwort abgelaufen oder initial ist. Je nachdem, ob sich der Nutzer interaktiv angemeldet hat oder nicht, muss das Kennwort geändert werden.

Systembenutzer

Systembenutzer sind Benutzer, die in technischen Abläufen, wie z. B. Batchläufen, Verwendung finden. Der Benutzer meldet sich hier nicht über das SAP GUI an. Beim Einsatz von Systembenutzern sind Mehrfachanmeldungen möglich. Für Kennwörter gibt es keine Änderungspflicht.

Referenzbenutzer

Der *Referenzbenutzer* ist ein Mittel, um die Berechtigungsadministration zu vereinfachen. Es ist nicht möglich, sich über einen solchen Benutzer am SAP-System anzumelden, sondern er dient lediglich dazu, Berechtigungen zu kopieren oder zu vererben.

Das betriebswirtschaftliche Berechtigungskonzept muss auch Aussagen zu den dargestellten Benutzern enthalten. Regelmäßig dürfen auch für technische Benutzer nur die Berechtigungen vergeben werden, die erforderlich sind. Umso mehr gilt dieses Prinzip für alle Benutzer, die Personen Zugriffe auf das System ermöglichen.

6.1.2 Benutzerpflege (ABAP)

Benutzerstammsatz

In der Benutzerpflege wird für jeden Benutzer in jedem Mandanten ein Benutzerstammsatz angelegt. Er besteht aus dem Benutzernamen, Daten zur Person, Einstellungen für den Benutzer, benutzerspezifi-

schen Parametern, den Berechtigungen aus Rollen und/oder Profilen und einigen weiteren Einstellungen. Der Benutzerstammsatz hat eine erhebliche Bedeutung für die Sicherheit und Ordnungsmäßigkeit des Systems. Sämtliche Protokollierungen von Systemzugriffen und in den Belegen beziehen sich auf den Benutzernamen. Diese Protokolle müssen je nach definierter Aufbewahrungsfrist langfristig aufbewahrt werden. Sie müssen darüber hinaus lesbar bleiben, und das bedeutet in diesem Kontext, dass der Benutzer gegebenenfalls auch nach zehn Jahren nachvollziehbar sein muss, der eine bestimmte Charge freigab oder einen Beleg buchte. Daraus ergibt sich zwingend und ausnahmslos, dass ein Benutzer nur einmalig einer Person zugeordnet werden darf. Benutzer zu »vererben«, also sie im Laufe der Zeit unterschiedlichen Mitarbeitern zur Verfügung zu stellen, ist in jedem Fall eine substanzielle Gefährdung der Sicherheit und Ordnungsmäßigkeit.

Eine Person – ein Benutzer

Auch die Praxis, eine Person im System mit mehreren Benutzern auszustatten, ist eine ähnlich erhebliche Gefährdung. Allerdings kann hier eine logische Ausnahme geltend gemacht werden, wie sie z. B. im Superuser Privilege Management (SPM) von SAP BusinessObjects Access Control möglich ist. Dort wird in einem definierten und protokollierten Verfahren aus dem »normalen« Benutzer heraus ein Superuser gestartet, der entsprechend weitreichende Berechtigungen hat. Generell gilt, wenn eine Person in einem System mehrere Benutzer hat, ist ein Nachweis etwaiger Funktionstrennungskonflikte und ebenso von Vorgängen unter Umgehung der Funktionstrennung konzeptionell nur mit erheblichem Aufwand, praktisch hingegen nicht mehr darstellbar. Auch in Bezug auf diese Praxis ist zumindest der Verdacht naheliegend, dass es sich um eine substanzielle Gefährdung der Sicherheit und Ordnungsmäßigkeit handelt. Die Eindeutigkeit der Zuordnung des Benutzers zur Person bezeichnen wir als *Identitätsprinzip*.

Kennwortregeln

In den meisten Organisationen werden nach wie vor fast täglich Benutzer und Kennwörter weitergegeben. Der einzig regelkonforme Umgang mit diesem Missbrauch ist, diesen dauerhaft zu unterbinden. Den Missbrauch können Sie einfach auswerten: Benutzer und Rechner können ohne Schwierigkeit ermittelt werden, ebenso kann ohne Schwierigkeiten festgestellt werden, welche Personen an einem

bestimmten Tag nicht arbeiten, bringt man diese Informationen zusammen, gelingt der konkrete Nachweis über missbräuchliche Nutzung von Benutzern. Datenschutzrechtliche Bedenken gegen dieses Verfahren können nicht geltend gemacht werden, da eine missbräuchliche Nutzung von Benutzern gegebenenfalls den Zugriff auf sensible Daten (und damit einen Verstoß gegen den Datenschutz) ebenso ermöglicht wie deutliche Gefährdungen des Belegprinzips. Neben einer einschlägigen Auswertung sollten immer auch arbeitsrechtliche Schritte erwogen werden. Die Kennwortregeln werden in Abschnitt 7.3, »Parameter für Kennwortregeln«, dargestellt.

Benutzerpflege vereinheitlichen

Das Verfahren der Benutzeranlage kann über SAP BusinessObjects Access Control, SAP NetWeaver Identity Management, die Zentrale Benutzerverwaltung (siehe für alle drei Lösungen Kapitel 10, »Zentrales Management von Benutzern und Berechtigungen«), vereinheitlicht und signifikant vereinfacht werden.

Vorgehen in der Benutzerpflege

Zum Anlegen oder Ändern eines Benutzers verwenden Sie die Transaktion SU01 (Benutzerpflege).

Beim Anlegen tragen Sie den gewünschten Benutzernamen im Feld Benutzer ein und klicken auf den Button Anlegen (siehe Abbildung 6.2). In den folgenden Bildschirmen werden die Angaben und Attribute des Benutzers gepflegt.

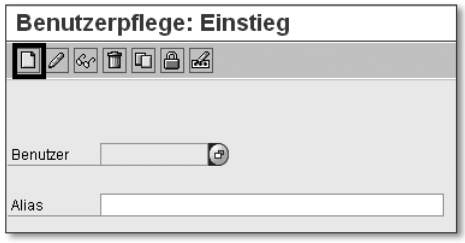


Abbildung 6.2 Einstieg in die Benutzerpflege

Registerkarte »Adresse«

Auf der Registerkarte Adresse (siehe Abbildung 6.3) müssen Sie mindestens die Angaben zur Person pflegen.

Registerkarte »Logondaten«

Danach pflegen Sie auf der Registerkarte Logondaten den Benutzertyp und abhängig vom Benutzertyp das Kennwort. In der Regel werden Sie den Dialogbenutzer pflegen.

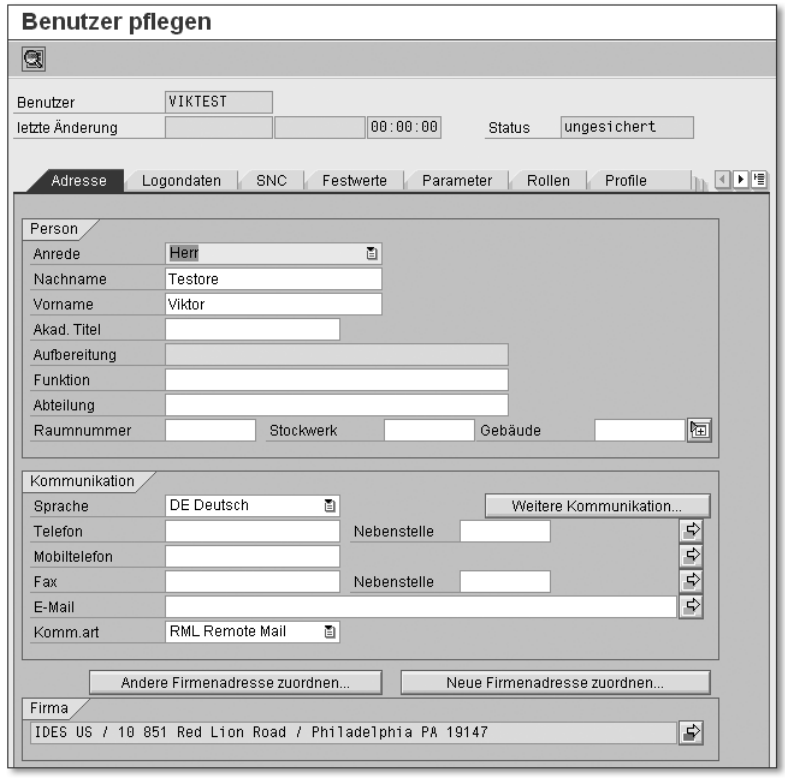


Abbildung 6.3 Registerkarte »Adresse« der Benutzerpflege

Das Kennwort können Sie automatisch generieren (Button WIZARD) oder manuell festlegen. Die Pflege einer Benutzergruppe für Berechtigungen ist dringend zu empfehlen, unter anderem um grundlegende Unterscheidungen zwischen Systemadministration und Endbenutzern zu ermöglichen. Neben der Benutzergruppe für Berechtigungsprüfungen können Benutzer beliebig vielen Gruppen zugeordnet werden (Registerkarte GRUPPEN). Dies dient u. a. der vereinfachten Pflege und Auswertung (siehe Abbildung 6.4).

Registerkarte »SNC«

Auf der Registerkarte SNC (*Secure Network Communications*) werden Angaben in Bezug auf ein (existierendes) Single-Sign-on-Verfahren (SSO) gepflegt. SNC ist für die Benutzerauthentifizierung verfügbar und stellt bei Verwendung des SAP GUI for Windows oder RFC eine SSO-Umgebung bereit.

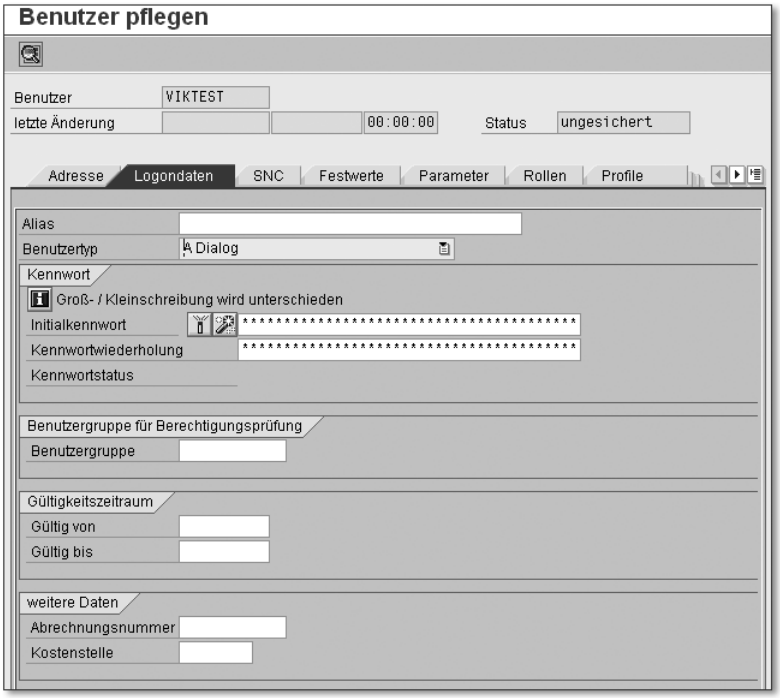


Abbildung 6.4 Pflege der Logon-Daten des Benutzers

Registerkarte »Festwerte«

Auf der Registerkarte FESTWERTE pflegen Sie Benutzerfestwerte, wie Startmenü, Drucker (Ausgabegerät), Dezimaldarstellung und Zeitzone.

Registerkarte »Parameter«

Parameter sind Angaben zum Benutzer, die ursprünglich dazu eingerichtet wurden, entsprechende Werte, wie z. B. den Buchungskreis, automatisch in die Selektion entsprechender Reports in FI zu übernehmen. Mittlerweile werden über Parameter aber auch Zugriffsmöglichkeiten unter anderem in ESS gesteuert, damit können Parameter fakultativ auch Zugriffsberechtigungen einschränken. Für die Parameter steht eine Werthilfe zur Verfügung (siehe Abbildung 6.5). Die einheitliche Betrachtung von Berechtigungen wird durch die Verwendung von Benutzerparametern erschwert.

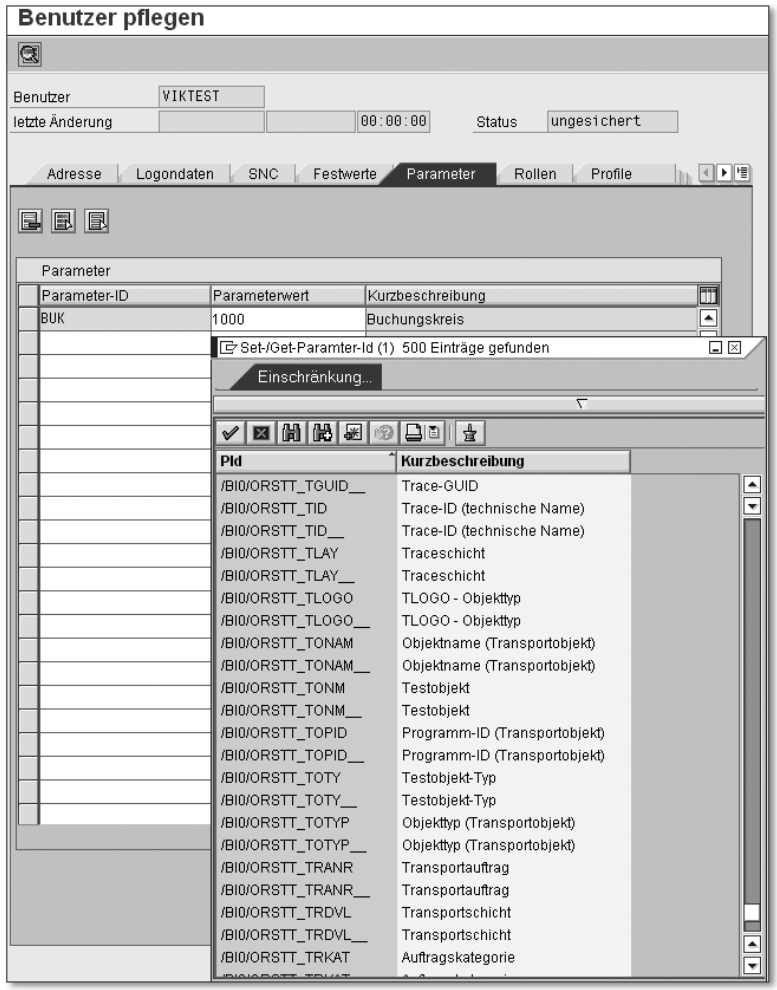


Abbildung 6.5 Registerkarte »Parameter«

Registerkarte »Rollen«

Auf der Registerkarte ROLLEN (siehe Abbildung 6.6) können dem Benutzer Rollen zugeordnet werden. Sofern Rollen zugeordnet sind, können sie direkt (durch Zuordnung einer Einzelrolle oder Sammelrolle) oder indirekt zugeordnet sein. Die indirekte Zuordnung erfolgt über das Organisationsmanagement von SAP ERP HCM (siehe Kapitel 8, »Rollenzuordnung über das Organisationsmanagement«).

Die unterschiedlichen Zuordnungen werden verdeutlicht durch unterschiedliche Icons in der Spalte TYP und durch unterschiedliche farbliche Codierungen, blau gekennzeichnete Rollen sind indirekt zugeordnet. Die direkt zugeordneten Rollen sind schwarz gekennzeichnet.

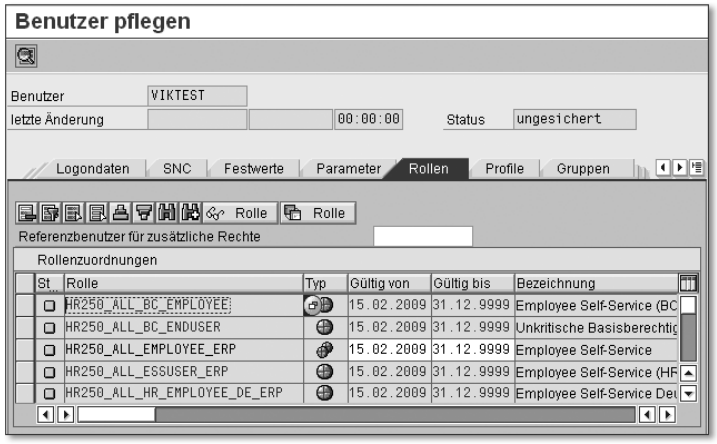


Abbildung 6.6 Registerkarte »Rollen«

Im Feld Referenzbenutzer für zusätzliche Rechte kann ein Referenzbenutzer eingetragen werden (siehe Abschnitt 6.1.1, »Benutzer«), dessen Zuordnungen hier (ergänzend) übernommen würden.

Registerkarte »Profile«

Auf der Registerkarte Profile (siehe Abbildung 6.7) sind die dem Benutzer zugeordneten Profile zusammengefasst. Ausnahmslos sollen sämtliche Profile eines Endbenutzers »Profile zur Rolle« sein. Prinzipiell stünde auf der Registerkarte Profile auch die Möglichkeit zur Verfügung, Profile manuell zuzuordnen. In Abschnitt 6.3.1, »Berechtigungsprofile«, wird dargestellt, warum die Profilpflege jedoch keine angemessene Option für die Verwaltung von Endbenutzerberechtigungen ist.

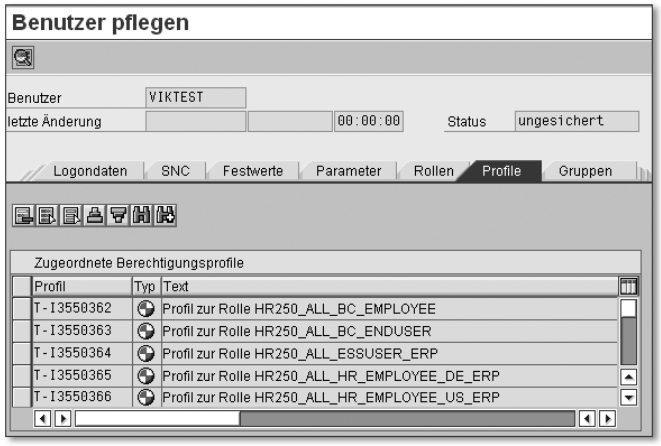


Abbildung 6.7 Registerkarte »Profile«

Dem Benutzer werden Rollen zugeordnet, diese enthalten Transaktionen und Berechtigungsobjekte, die wir im nächsten Abschnitt darstellen werden.

6.2 Transaktion – Programm – Berechtigungsobjekt

In diesem Abschnitt werden wir Ihnen den Zusammenhang von Transaktionen und Programmen, die Logik der Berechtigungsprüfung und die Ausprägung der Berechtigungen durch Berechtigungsobjekte erläutern.

Berechtigungen dienen dazu, Programme in einer definierten Tiefe ausführen zu können. Jede Programmausführung durch einen Dialogbenutzer sollte über eine Transaktion erfolgen. ECC 6.0 verfügt über mehr als 370.000 Programme und mehr als 70.000 Transaktionen.

6.2.1 Transaktion

Über einen Transaktionscode wird im SAP-System eine betriebswirtschaftliche Funktion (eine sogenannte *Transaktion*) im System ausgeführt. Entsprechend ist ein Großteil der Transaktionen auch in Bezug auf die ursprünglichen Module fachlich gruppiert und im SAP Easy Access-Menü enthalten (siehe Abbildung 6.8)

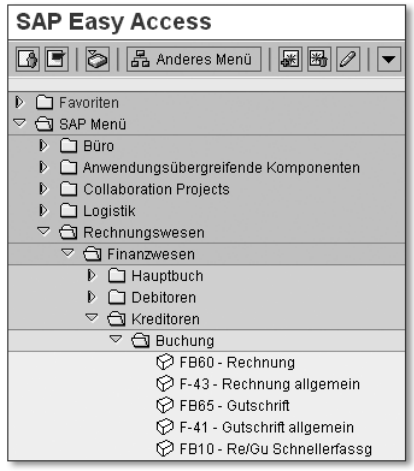


Abbildung 6.8 Transaktionen im SAP Easy Access-Menü

Eine Transaktion ist grundsätzlich mit einem ausführbaren Programm verbunden. Die Zuordnung einer Transaktion zu einem Programm dient bereits der Einschränkung von Berechtigungen. Programme können entsprechend über die Transaktion oder aber über die direkte Programmausführung mit der Transaktion SA38 (ABAP/4-Reporting) ausgeführt werden:

- Um ein Programm über eine Transaktion ausführen zu können, braucht der Benutzer minimal die Berechtigung, die Transaktion aufrufen zu dürfen. Diese Berechtigung wird im Berechtigungsobjekt S_TCODE (Transaktionscode-Prüfung bei Transaktionsstart) hinterlegt. Es handelt sich somit um eine spezifische Berechtigung zur Ausführung einer bestimmten Transaktion. Diese wird meistens noch weiter über Berechtigungsobjekte eingeschränkt.
- Um ein Programm über die Transaktion SA38 (ABAP/4-Reporting) ausführen zu können, braucht der Benutzer die Berechtigung für die SA38, die auch im S_TCODE hinterlegt wird. Es handelt sich somit um eine unspezifische Berechtigung für das Ausführen aller Programme. Diese wird noch weiter über Berechtigungsobjekte eingeschränkt.

Eingangsprüfung

Der Transaktion kann eine weitere Eingangsprüfung zugeordnet sein, die als zusätzliche sehr allgemeine Berechtigungsprüfung nach der Prüfung auf der Transaktionsberechtigung wirkt. Sie ist keine detaillierte Prüfung im Programmablauf, sondern es wird lediglich erreicht, dass die definierten Werte als Berechtigung vorhanden sein müssen. Eine logische Verbindung zu den Daten gibt es nicht.

Beispiel

Wenn als Eingangsprüfung ein kundeneigenes Berechtigungsobjekt Z_ALLES_GUT mit dem Feld ALLES_GUT und dem Wert »Y« definiert ist, müssen genau diese Berechtigungen auch im Benutzerpuffer vorhanden sein, unabhängig davon, dass Z_ALLES_GUT in keinem Programm als Berechtigungsprüfung definiert ist.

Die Eingangsprüfung wird in der Transaktion SE93 (Pflege Transaktionscodes) festgelegt (siehe Abbildung 6.9).

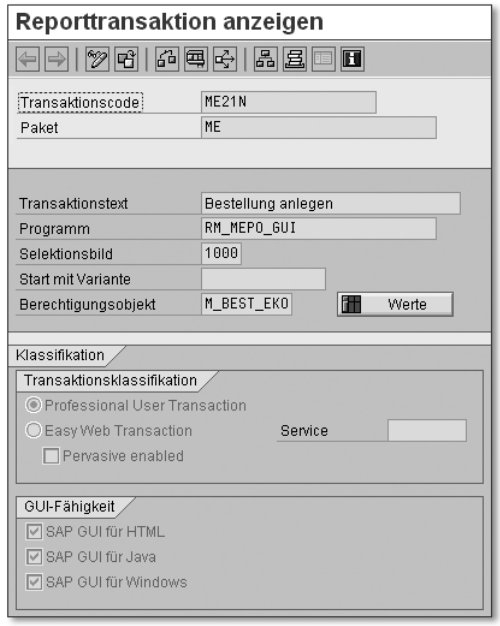


Abbildung 6.9 Berechtigungsobjekt als Eingangsprüfung

6.2.2 Prüfung im Programmablauf

Im Programmablauf prüft das System, ob die für die Transaktion benötigten Werte denen im Benutzerpuffer entsprechen. Im Benutzerpuffer befinden sich meistens gleiche Berechtigungsobjekte in unterschiedlicher Ausprägung. Als Berechtigung wird das Berechtigungsobjekt betrachtet, das die am besten passende Ausprägung hat. Das ist wichtig für die Logik von Rollen: Geprüft wird jeweils gegen das für den Anwendungsfall am weitesten berechtigte Berechtigungsobjekt – ohne Relation zur Transaktion.

Prüfung bei Aufruf einer Transaktion

Beim Aufruf einer Transaktion wird immer zunächst das Berechtigungsobjekt S_TCODE (Transaktionscode-Prüfung bei Transaktionsstart) abgeprüft. Danach können nahezu beliebig viele weitere Prüfungen vorgesehen sein. Dies ist unmittelbar abhängig vom jeweiligen Programm. Im Quellcode ist die jeweilige Prüfanweisung festgelegt als Check eines Berechtigungsobjekts und seiner Felder – dabei müssen nicht alle Felder eines Berechtigungsobjekts verprobt werden. Der entsprechende String der Prüfanweisung ist `authority-check` (siehe Abbildung 6.10).

Dabei kann die Prüfung im unmittelbar verbundenen Programm oder in Includes enthalten sein. Die Prüfung findet regelmäßig über *Feldwerte* in *Berechtigungsobjekten* statt. Im Programm findet sich ein Authority-Check. In Abbildung 6.10 ist exemplarisch eine Prüfung auf das Berechtigungsobjekt S_TABU_DIS (Tabellenpflege (über Standardtools wie z. B. die Transaktion SM30)) dargestellt. Nur wenn der Benutzer die Berechtigungen für das Objekt mit den definierten Feldwerten hat (Felder DIBERCLS und ACTVT), darf er den definierten Programmschritt vollziehen.

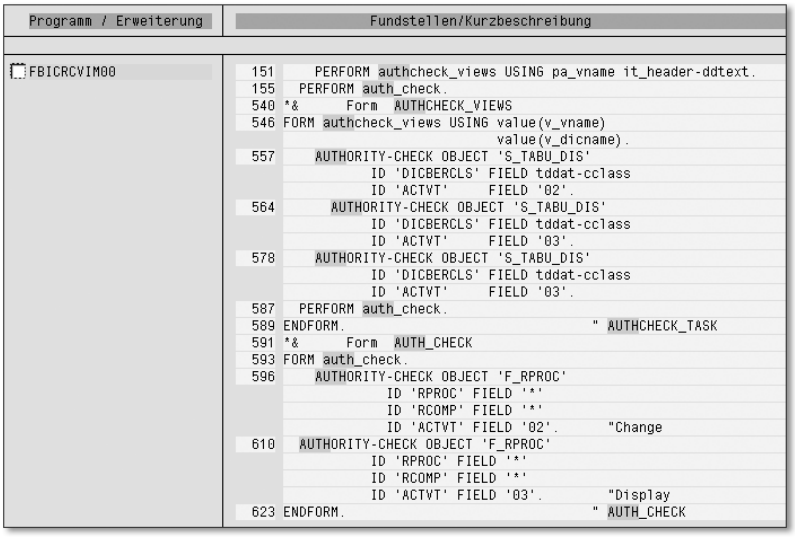


Abbildung 6.10 Authority-Check in einem Programm

Die in Abbildung 6.11 gezeigte Prüfung ist eine stark vereinfachte Prüfung. Deutlich werden soll, dass es Prüfungen beim Aufruf eines Programms und bei seiner weiteren Ausführung gibt. Es gibt Programme, die sehr detailliert Berechtigungen für diverse funktionale und organisatorische Unterscheidungsmerkmale abprüfen (z. B. in der Kostenstellenrechnung Berichte, die für jede Kostenstelle, jede Kostenart einzeln prüfen). Es gibt andere, die keine Prüfung enthalten. Die detaillierte Prüfung auf eines oder mehrere konkrete Merkmale unterscheidet viele Berechtigungsprüfungen im Programmablauf von der Eingangsprüfung.

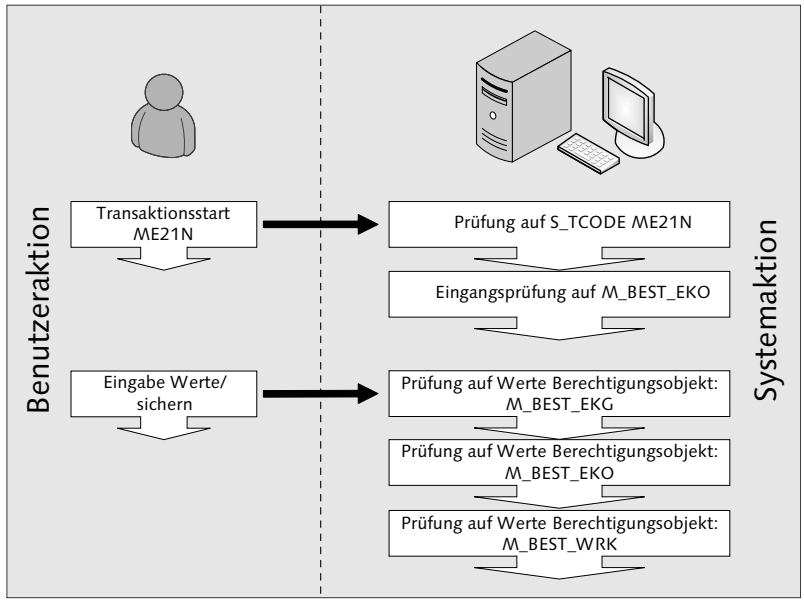


Abbildung 6.11 Prüfung im Programmablauf

6.2.3 Berechtigungsobjekt

Der zentrale Begriff des technischen Berechtigungskonzepts in ABAP ist das *Berechtigungsobjekt* (siehe Abbildung 6.11). Es besteht aus einer Kombination von Berechtigungsfeldern, die einzelne Berechtigungen definieren. Diese stellen die feinteiligste Ebene der Berechtigungsdifferenzierung bereit. Tatsächlich sind in der Programmablaufprüfung meist Checks auf bestimmte Werte von Berechtigungsfeldern bestimmter Berechtigungsobjekte definiert.

Berechtigungsobjekte sind sehr unterschiedlich angelegt. Oft bestehen sie aus Aktivitäten einerseits und organisatorischen Beschränkungen wie z. B. Belegart oder Kostenstelle andererseits. Das Berechtigungsobjekt enthält höchstens zehn Berechtigungsobjektfelder. Diese Felder sind mit im ABAP Dictionary abgelegten Datenelementen verbunden.

In Abbildung 6.12 ist ein sehr einfaches Beispiel eines Berechtigungsobjekts dargestellt. Deutlich komplexer ist das Berechtigungsobjekt P_ORGIN (HR: Stammdaten), das sieben Felder enthält und in Abbildung 6.13 zu sehen ist. Von den sieben Feldern sind sechs organisatorischer Art.

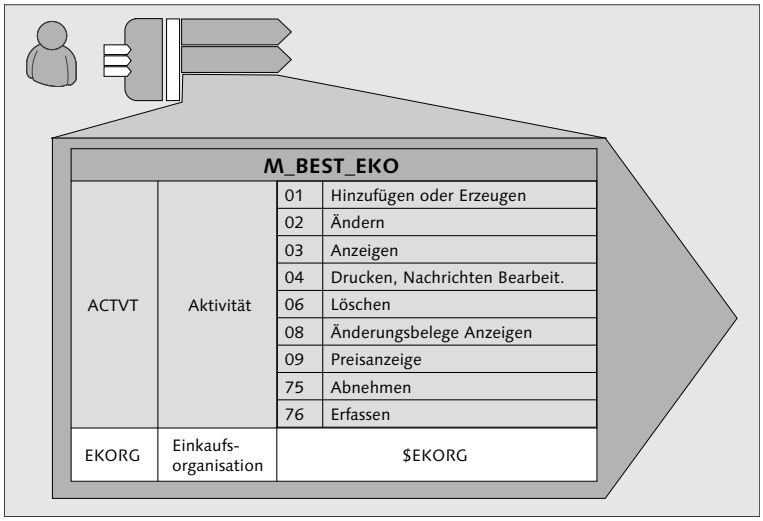


Abbildung 6.12 Berechtigungsobjekt M_BEST_EKO (Einkaufsorganisation in Bestellung)

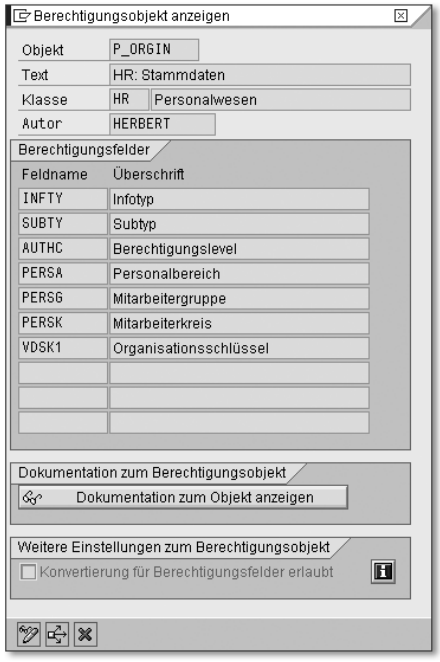
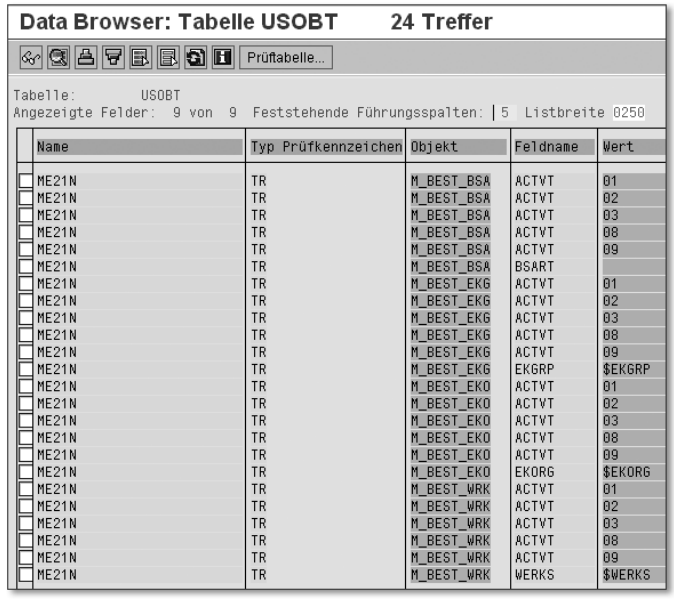


Abbildung 6.13 Berechtigungsobjekt P_ORGIN (HR: Stammdaten)

Verallgemeinernd kann gesagt werden, dass die meisten Berechtigungsobjekte aus einem oder mehreren organisatorischen Attributen

(aufbau- oder ablauforganisatorisch) und einer Definition möglicher Aktivitäten bestehen. Im einfachen Beispiel des Berechtigungsobjekts M_BEST_EKO (Einkaufsorganisation in Bestellung) wird das Attribut EINKAUFSORGANISATION mit verschiedenen möglichen Aktivitäten, wie z. B. HINZUFÜGEN, kombiniert. Für den Fall, dass ein Benutzer nur eine Rolle mit genau der Transaktion ME21N (Bestellung anlegen) bekäme, würde dieses Berechtigungsobjekt festlegen, in welcher Einkaufsorganisation er eine bestimmte Aktivität ausführen darf. In Kapitel 3, »Organisation und Berechtigungen«, wurden die Organisationsebenen und mögliche Verbindungen von Organisationsebenen dargestellt. Die Einkaufsorganisation ist eine Organisationsebene.

Neben der Einkaufsorganisation werden bei der Bestellung standardmäßig auch noch das Werk (Feld WERKS) und die Einkäufergruppe (Feld EKGRP) als Organisationsebenen abgeprüft (siehe Abbildung 6.14). Damit stehen drei Organisationsebenen mit primär aufbauorganisatorischem Bezug für die Differenzierung zur Verfügung. Es kann also – solange diese Organisationsebenen aus Sicht des Berechtigungskonzepts auch sinnvoll genutzt werden – punktgenau festgelegt werden, in welchem Werk, welcher Einkäufergruppe und welcher Einkaufsorganisation ein Benutzer eine Bestellung anlegen darf.



Data Browser: Tabelle USOBT 24 Treffer

Prüftabelle...

Tabelle: USOBT
Angezeigte Felder: 9 von 9 Feststehende Führungsspalten: 5 Listbreite 0250

Name	Typ Prüfkennzeichen	Objekt	Feldname	Wert
ME21N	TR	M_BEST_BSA	ACTVT	01
ME21N	TR	M_BEST_BSA	ACTVT	02
ME21N	TR	M_BEST_BSA	ACTVT	03
ME21N	TR	M_BEST_BSA	ACTVT	08
ME21N	TR	M_BEST_BSA	ACTVT	09
ME21N	TR	M_BEST_BSA	BSART	
ME21N	TR	M_BEST_EKG	ACTVT	01
ME21N	TR	M_BEST_EKG	ACTVT	02
ME21N	TR	M_BEST_EKG	ACTVT	03
ME21N	TR	M_BEST_EKG	ACTVT	08
ME21N	TR	M_BEST_EKG	ACTVT	09
ME21N	TR	M_BEST_EKG	EKGRP	$EKGRP
ME21N	TR	M_BEST_EKO	ACTVT	01
ME21N	TR	M_BEST_EKO	ACTVT	02
ME21N	TR	M_BEST_EKO	ACTVT	03
ME21N	TR	M_BEST_EKO	ACTVT	08
ME21N	TR	M_BEST_EKO	ACTVT	09
ME21N	TR	M_BEST_EKO	EKORG	$EKORG
ME21N	TR	M_BEST_WRK	ACTVT	01
ME21N	TR	M_BEST_WRK	ACTVT	02
ME21N	TR	M_BEST_WRK	ACTVT	03
ME21N	TR	M_BEST_WRK	ACTVT	08
ME21N	TR	M_BEST_WRK	ACTVT	09
ME21N	TR	M_BEST_WRK	WERKS	$WERKS

Abbildung 6.14 Objekt- und Feldvorschlagswerte für die Transaktion ME21N (Bestellung anlegen)

In jedem Fall kann davon ausgegangen werden, dass eine sicher programmierte Transaktion für einen komplexen betriebswirtschaftlichen Vorgang immer eine Prüfung verschiedener Berechtigungsobjekte beinhaltet. Umgekehrt ist es allerdings auch so, dass ein Berechtigungsobjekt in mehreren Transaktionen enthalten ist. Das Berechtigungsobjekt M_BEST_EKO (Einkaufsorganisation in Bestellung) ist als Standardvorschlag mit 148 Transaktionen verbunden (siehe Abbildung 6.15).

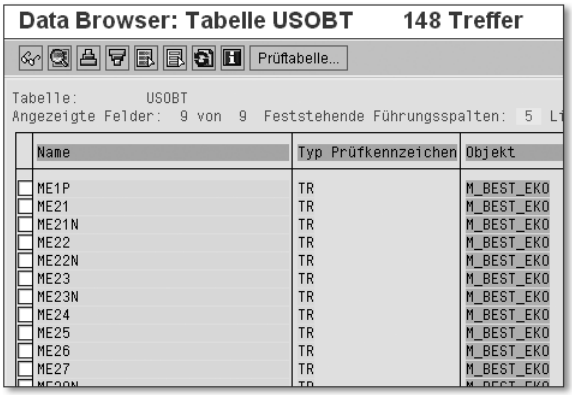


Abbildung 6.15 Vorschlag Berechtigungsobjekt »Einkaufsorganisation in Bestellung« (Objekt M_BEST_EKO) in Transaktionen

Relation von Berechtigungsobjekt und Transaktion

Die Berechtigung einer Transaktion wird regelmäßig durch mehrere Berechtigungsobjekte ausgesteuert. Ein Berechtigungsobjekt steuert regelmäßig mehrere Transaktionen aus. Somit ergeben sich folgenden Relationen:

- Eine Transaktion kann mit n Berechtigungsobjekten verbunden sein.
- Ein Berechtigungsobjekt kann mit n Transaktionen verbunden sein.

In SAP ERP 6.0 stehen circa 1.000 Berechtigungsobjekte zur Verfügung. Diese sind Klassen zugeordnet. Die Klassen entsprechen in Grundzügen den früher so genannten *SAP-Modulen*. Die Klassen können in der Tabelle TOBC (Klasseneinteilung der Berechtigungsobjekte) ausgewertet werden. Die mehr als 100.000 Transaktionen (alle eingeschlossen) werden durch circa 1.000 Berechtigungsobjekte ausgesteuert, dabei ist eine n:n-Relation möglich.

Durch die hohe (und wachsende) Integration werden Berechtigungsobjekte einer Komponente (wie z. B. Innenaufträge (CO-OM-OPA)) auch in anderen Komponenten genutzt, da teilweise auf dieselben Datenstrukturen zurückgegriffen wird. Andererseits eröffnet das Customizing die Möglichkeit, Prüfungen auf Daten, die primär anderen Komponenten zugeordnet sind, vorzunehmen (bei der Bestellung kann auf das Sachkonto geprüft werden, oder alle Kontierungen einer Bestellung können auf die Kontierungsobjekte des SAP Haushaltsmanagements geprüft werden). Schließlich – das gilt insbesondere für die Entwicklung kundeneigener Programme – können Berechtigungsobjekte relativ frei in eigenentwickelte Programme aufgenommen werden.

Notwendigkeit individueller Ermittlung

Da das technische Berechtigungskonzept nicht in einem homogenen Vorgehen, sondern problembezogen von unterschiedlichen Akteuren (bei SAP und außerhalb) weiterentwickelt wurde, sind die Unterschiede zwischen den Berechtigungsobjekten verschiedener Komponenten und sogar innerhalb einer Komponente nur noch historisch zu erklären. Wie in Abschnitt 6.4, »Analyse von Berechtigungsprüfungen«, gezeigt werden soll, müssen deswegen (und aus den bereits angeführten Gründen wie Customizing, optionale Prüfungen, Komponentenintegration) die notwendigen Details eines Prüfungsablaufs »individuell« (d. h. Transaktion für Transaktion) ermittelt werden.

Berechtigungsobjekte: optionale Berechtigungsprüfung

In einigen Fällen sind Berechtigungen als optionale Prüfung vorgesehen. So können z. B. Kreditoren durch eine Berechtigungsgruppe geschützt werden (in diesem Fall zu verstehen als zusätzliches Attribut auf einem Stammdatum). Erst wenn sie eine Berechtigungsgruppe ausweisen, wird gegen das zugehörige Berechtigungsobjekt verprobt. Die optionale Prüfung wird in Abschnitt 7.5.1, »Optionale Berechtigungsprüfungen auf Berechtigungsgruppen«, behandelt.

Berechtigungsprüfung und Customizing im Modul

Regelmäßig können Berechtigungen vom Customizing abhängen. Dies gilt für Grundeinstellungen ebenso wie für Gruppierungen oder Zuordnungen. An verschiedenen Stellen sind Eingriffe in das Customizing in diesem Buch dargestellt (u. a. in Kapitel 7 und 18). Konkret kann durch das modulbezogene Customizing die Berechtigungsprüfung um weitere Berechtigungsprüfungen ergänzt werden. Der Zusammenhang zwischen Customizing und Berechtigungen wird in den jeweiligen Kapiteln zu den Applikationen entwickelt.

6.3 Rollen und Rollenprofile

In SAP ERP gibt es unterschiedliche Möglichkeiten, einem Benutzer Berechtigungen zuzuordnen. Die Methode der Wahl für die Zuweisung von Berechtigungen an Endbenutzer ist ein rollenbasiertes Konzept unter Nutzung des Profilgenerators. In Abschnitt 6.3.1, »Berechtigungsprofile«, gehen wir zunächst auf die veraltete Pflege von Profilen ein. Anschließend wird detailliert dargestellt, wie Sie bei der Pflege von Rollen verfahren sollten.

6.3.1 Berechtigungsprofile

Manuell erzeugte Berechtigungsprofile sind vor der Einführung des Profilgenerators mit Release SAP R/3 3.1 die Container für Berechtigungen gewesen, die einem Benutzer zugeordnet wurden. SAP empfiehlt die Pflege über den Profilgenerator, Transaktion PFCG (Pflege von Rollen) (siehe Abbildung 6.16). Die alte Transaktion zur Pflege von Profilen ist SU02 (Manuelle Pflege von Profilen).

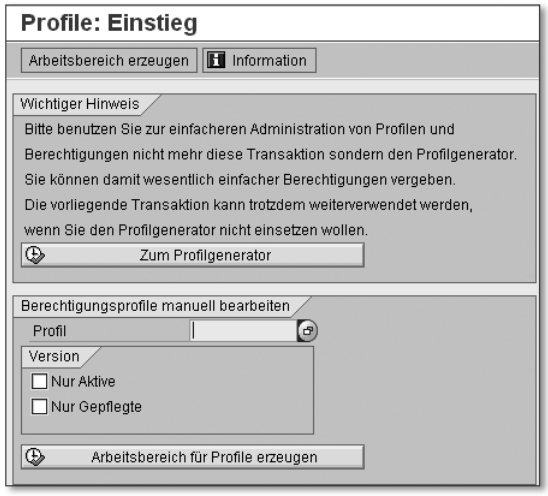


Abbildung 6.16 Einstieg in die manuelle Profilpflege

Nach dem Einstieg muss Berechtigungsobjekt für Berechtigungsobjekt und Feld pro Berechtigungsobjekt für Feld pro Berechtigungsobjekt manuell eingetragen werden, welche Berechtigungen ein Berechtigungsprofil enthalten soll (siehe Abbildung 6.17). Das ist einerseits mühsam, andererseits wird in dieser Funktion nicht die Pflege über

Vorschlagswerte unterstützt. Die Pflege über Vorschlagswerte (siehe Kapitel 7, »Systemeinstellungen und Customizing«) ist nicht nur eine signifikante Vereinfachung der Berechtigungspflege, sie unterstützt darüber hinaus auch die Pflege während eines Upgrades, und letztlich ist sie als vorgabeorientierte Pflege von Berechtigungen einzig in der Lage, einen positiven Ausweis von Regelkonformität zu leisten.

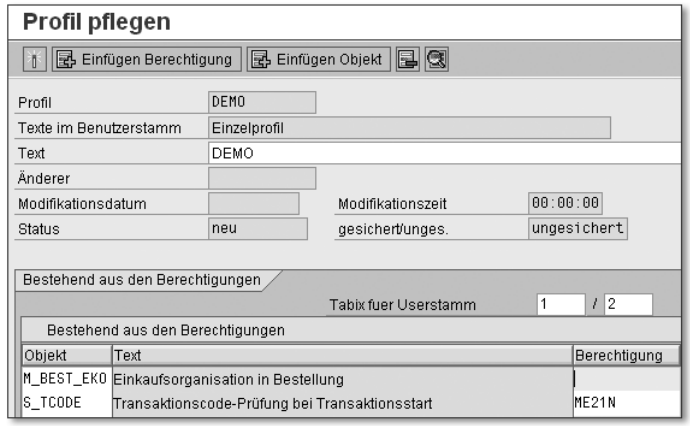


Abbildung 6.17 Pflege eines Berechtigungsprofils

Profilbasierte Berechtigungskonzepte sind nicht compliant

Ein Berechtigungskonzept auf der Grundlage manueller Profile ist ineffizient in der Pflege, kostentreibend im Upgrade und erfüllt nicht den Anspruch, auf der Grundlage einheitlicher Vorgaben Berechtigungen zu vergeben. Ein profilbasiertes Berechtigungskonzept läuft den anerkannten Best Practices der Berechtigungspflege in SAP-Systemen und einem positivem Compliance-Ansatz zuwider.

6.3.2 Anlage und Pflege von Rollen

Eine SAP-Rolle ist, technisch gesehen, eine Abstraktion. Sie dient der vereinfachten Erstellung, Ausprägung und Vergabe von Berechtigungen. Im Folgenden werden wir beschreiben, wie Sie beim Pflegen einer Rolle vorgehen sollten.

Festlegen von Rollenattributen

Die Rolle wird mit dem Profilgenerator über die Transaktion PFCG (Pflege von Rollen) angelegt, geändert, in einen Transportauftrag aufgenommen und gegebenenfalls einem Benutzer zugeordnet. Dabei werden zunächst der Rollenname, Beziehungen zu anderen Rollen und eine Beschreibung festgelegt (siehe Abbildung 6.18). Diese können auch als Attribute verstanden werden. Die Sichtweise von Rolle-

nattributen entspricht auch dem Vorgehen bei SAP BusinessObjects Access Control (siehe Kapitel 12, »SAP BusinessObjects Access Control«), dort ist die Attributierung allerdings sehr viel detaillierter möglich.

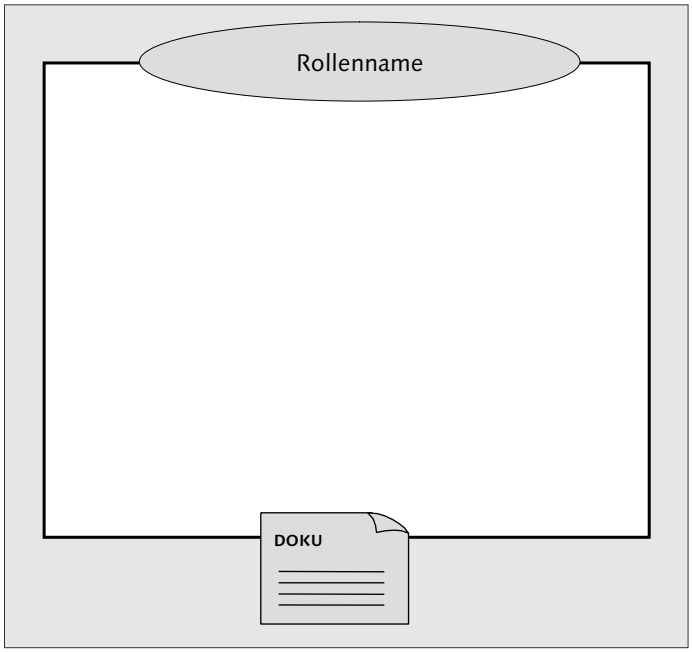


Abbildung 6.18 Erster Schritt: Festlegen von Rollenattributen

Zunächst muss ein eindeutiger Rollenname angegeben werden (siehe Abbildung 6.19). Dieser ist regelmäßig davon abhängig, welcher Rollentyp (siehe Abschnitt 6.5, »Weitere Rollentypen in SAP ERP«) genutzt werden soll. Im Einstiegsbildschirm erfolgt der Einstieg in die Pflege einer Einzelrolle oder einer Sammelrolle über die gleichnamigen Buttons.

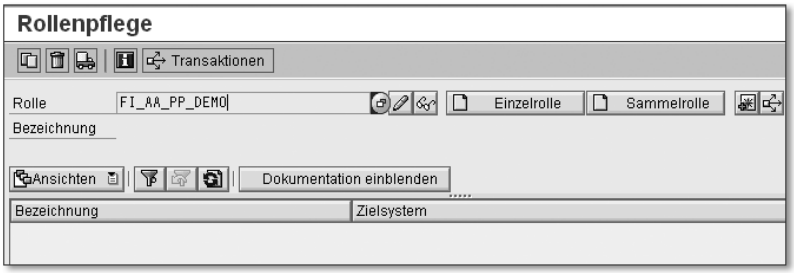


Abbildung 6.19 Einstiegsbildschirm des Profilgenerators

Exkurs: Namenskonvention der Rollen

Eine gute Namenskonvention stellt im Rollennamen alle Informationen bereit, die zur Analyse des Berechtigungskonzepts und zur vereinfachten Zuordnung von Rollen zu Benutzern beitragen. Dementsprechend gibt es nur fallweise richtige Namenskonventionen, aber keine, die für alle Kunden passt. In unserer Beratungspraxis verwenden wir die folgenden Kriterien für Rollennamen:

- Bündelungsfunktion: Sammelrolle/Einzelrolle
- Kennzeichner Komponente
- Kennzeichner Berechtigungsfunktion: funktionale Rolle/Wertrolle
- Kennzeichner Ableitung: Referenzrolle/abgeleitete Rolle/Einzelrolle
- Rollenbezeichner: Freitext
- Organisationskennzeichner: Kostenstelle/Auftrag o. Ä.

Funktionale Rolle, *Referenzrolle* und *abgeleitete Rolle* sind Begriffe, die den jeweiligen konzeptionellen Ansätzen entlehnt sind, die auch in Abschnitt 6.5, »Weitere Rollentypen in SAP ERP«, behandelt werden.

Die Reihenfolge der Kriterien ist abhängig von der weiteren Verwendung. Ein Präfix im Kundennamenraum ist nicht erforderlich. Nur das SAP-Präfix »SAP« und das Präfix »/« dürfen nicht verwendet werden.

Profilgenerator: Registerkarte »Beschreibung«

Wie in Abbildung 6.19 zu sehen ist, müssen Sie zunächst einen Rollennamen angeben, danach erreichen Sie über den Button Einzelrolle die Registerkarte Beschreibung (siehe Abbildung 6.20).

Abbildung 6.20 Profilgenerator: Registerkarte »Beschreibung«

Im Feld Beschreibung des Kopfbereichs kann eine allgemeine Beschreibung eingetragen werden. Erfahrungsgemäß sollte hier ein sprechender Text verwendet werden wie etwa »Kreditorenbuchhalter – interne Kreditoren«.

Auf der Registerkarte Beschreibung sollten Sie eine konkretisierende Beschreibung im Sinne einer Dokumentation und fakultativ einer Rollenänderungsverlaufsdokumentation eintragen. Erfahrungsgemäß sollten an dieser Stelle Besonderheiten festgehalten werden, z. B. besondere Verwendungen (wie: Rolle für Jahresabschluss) oder besondere Ausprägungen (wie: Ausprägung für Belegart AAA). Beim Anlegen der Rolle, und nur dann, kann eine Ableitungsbeziehung definiert werden.

Um die weiteren Registerkarten zu erreichen, müssen Sie beim Anlegen der Rollen an diesem Punkt die Rolle sichern.

Profilgenerator: Registerkarte »Menü«

Auf der Registerkarte Menü erfolgt die Festlegung, welche Transaktionen, Webservices und weiteren Objekte zur Rolle gehören. Dies ist in Abbildung 6.21 dargestellt. Alle Transaktionen werden im Menü aufgenommen.

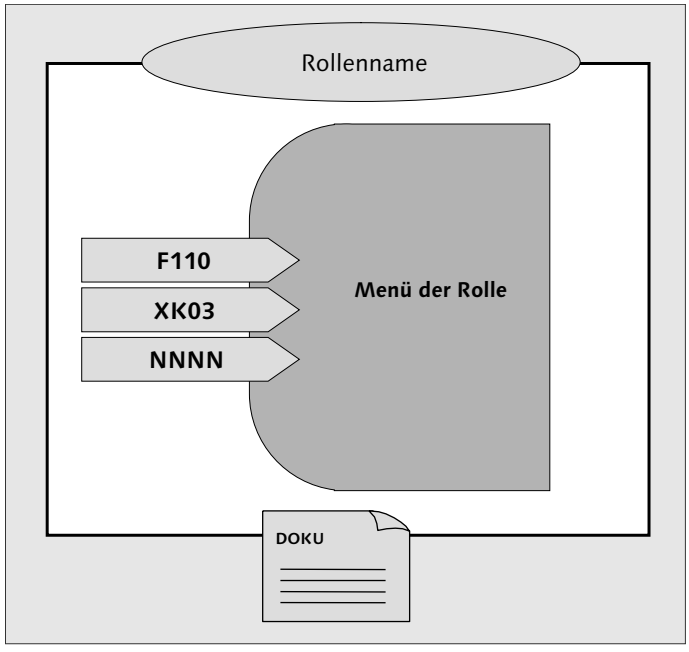


Abbildung 6.21 Festlegung des transaktionalen Rahmens einer Rolle

Letztlich ist dies die funktionale Verwendungsbestimmung der Rolle. Aus diesem und später dargestellten Gründen (Abschnitt 7.1, »Pflege und Nutzung der Vorschläge für den Profilgenerator«) sollten immer und ausnahmslos alle Transaktionen in das Menü eingetragen werden.

Abbildung 6.22 Profilgenerator: Registerkarte »Menü«

Auf der Registerkarte Menü können Transaktionen, Berichte, Webadressen, Dateien und weitere Objekte hinzugefügt werden. Dabei ist die Pflege des Menüs abhängig vom zugrunde liegenden Menükonzept. In Kapitel 7, »Systemeinstellungen und Customizing«, gehen wir auf mögliche Menükonzepte und deren Einstellung ein.

Im einfachsten Fall ordnen Sie Transaktionen über den Button Transaktion zu. Dieser ordnet die Transaktion in der Menüebene zu, in der Sie gerade aktiv sind (markierter Ordner). Tatsächlich ist dieser Weg nur dann sinnvoll, wenn es kein Menükonzept gibt oder wenn die Transaktion manuell genau in den Menüordner eingefügt wird, der vom Menükonzept dafür vorgesehen ist.

Die direkte manuelle Zuordnung von Transaktionen auf dem in Abbildung 6.23 gezeigten Weg muss in jedem Fall der Logik des Menükonzepts folgen.

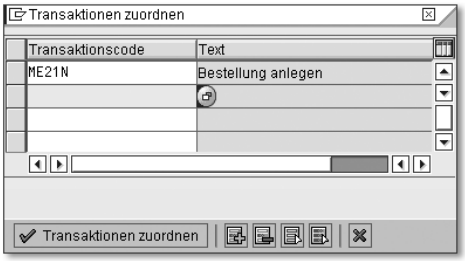


Abbildung 6.23 Profilgenerator, Registerkarte »Menü«: Transaktion zuordnen

Sofern ein Menükonzept besteht, sollten Sie die Pflege über den Button Aus dem SAP Menü oder Aus anderer Rolle oder Aus Bereichsmenü vorziehen (siehe Abbildung 6.24).

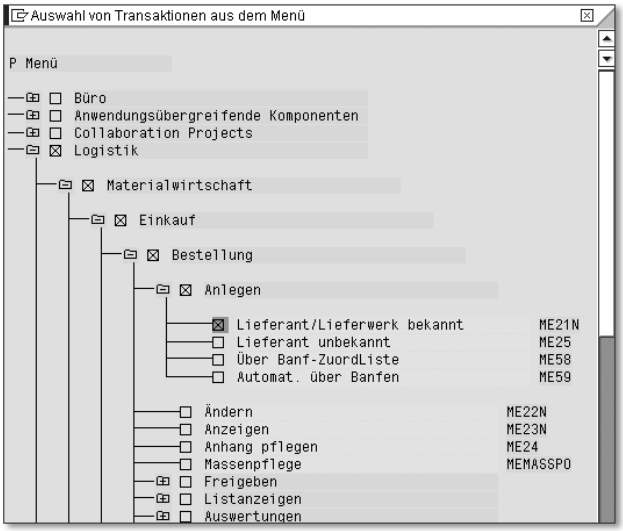


Abbildung 6.24 Profilgenerator, Registerkarte »Menü«: aus dem SAP-Menü zuordnen

Oftmals sollen im Benutzermenü eines Benutzers bestimmte Transaktionen, über die er verfügen muss, unsichtbar sein. Es handelt sich dabei um Transaktionen, die häufig (technisch nicht ganz korrekt) als »Hintergrundtransaktionen« bezeichnet werden. So ist es z. B. in Berichten häufig so, dass es diverse Absprünge in weitere Transaktionen gibt, die notwendig sind. Diese Transaktionen können über den Button Berechtigungsvorschlag (siehe Abbildung 6.22) eingefügt werden. Nach einem Klick auf den Button erscheint der in Abbildung 6.25 dargestellte Bildschirm, in dem der jeweilige Berechtigungsvorschlag gepflegt werden kann.

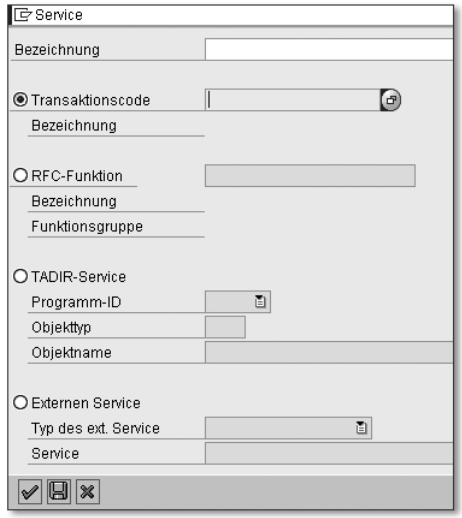


Abbildung 6.25 Profilgenerator, Registerkarte »Menü«: Berechtigungsvorschlag

Dieses Vorgehen bewirkt:

- dass Transaktionen nicht mehr manuell in das Berechtigungsobjekt S_TCODE (Transaktionscode-Prüfung bei Transaktionsstart) S_TCODE aufgenommen werden müssen, um sie »zu verbergen«
- dass die Vorschlagswerte der Transaktion USOBT_C ((Relation Transaktion → Ber.objekt (Kunde)) (siehe Kapitel 7, »Systemeinstellungen und Customizing«) übernommen werden
- dass diejenigen Berichte des Benutzerinformationssystems (Transaktion SUIM), die auf Transaktionen im Menü referenzieren, die vergebenen Transaktionen vollständig ausweisen

Abbildung 6.26 zeigt die Transaktion ME21N (Bestellung anlegen) als Berechtigungsvorschlag im Menü.

Über die Eingabe Zielsystem können Sie ein anderes System festlegen, in dem die Transaktionen der Rolle ausgeführt werden sollen. Dabei sollten möglichst nur RFC-Destinationen basierend auf dem Trusted-System-Konzept genutzt werden, sofern Sie über das SAP Easy Access-Menü im SAP GUI navigieren wollen.

Für weitere Funktionen auf der Registerkarte verweisen wir auf die SAP-Onlinehilfe.

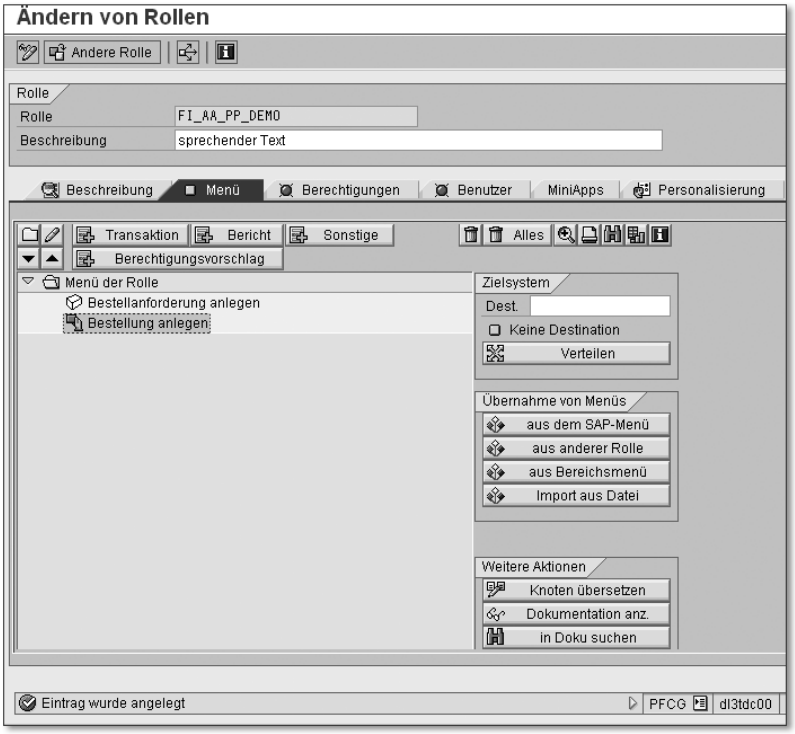


Abbildung 6.26 Profilgenerator, Registerkarte »Menü«: Berechtigungsvorschlag im Menü

Registerkarte »Berechtigungen«

Über die Registerkarte Berechtigungen findet die tatsächliche Pflege von Berechtigungen statt. Im Bereich Informationen zum Berechtigungsprofil können ein Profilname und ein Profiltext gepflegt werden. Meistens wird der Vorschlag unverändert übernommen, da die Zuordnung dieser Profile über die Rolle erfolgt und somit auch Auswertungen rollenbezogen und nicht mehr profilbezogen stattfinden.

Im Bereich Berechtigungsdaten pflegen und Profile generieren stehen Ihnen zwei Buttons zur Verfügung, der Button Berechtigungsdaten ändern und der Button Expertenmodus zur Profilgenerierung.

Beim Anlegen einer Rolle und dem erstmaligen Anlegen des Profils gibt es keinen Unterschied zwischen den beiden Buttons. In beiden Fällen gleicht der Profilgenerator die im Menü vergebenen Transaktionen mit den Vorschlagswerten für den Profilgenerator, Tabelle USOBT_C (Relation Transaktion → Ber.objekt (Kunde)) ab.

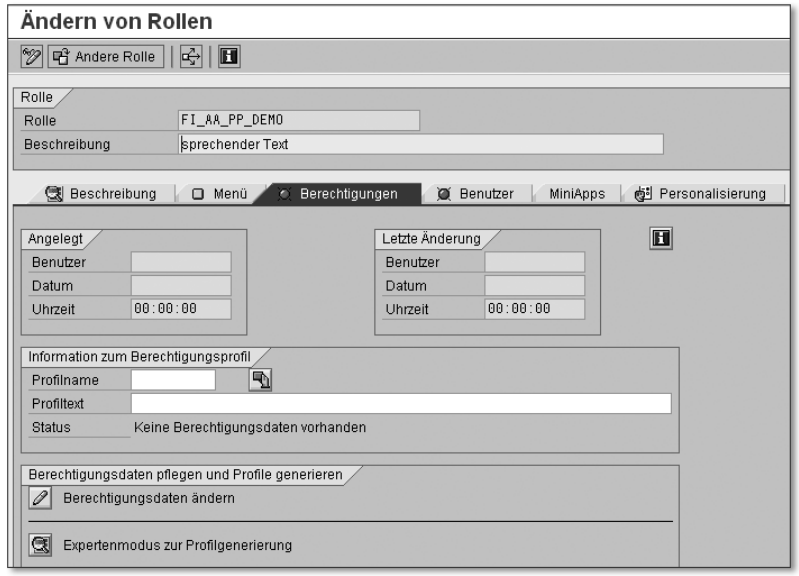


Abbildung 6.27 Profilgenerator: Registerkarte »Berechtigungen«

Der Unterschied wird erst relevant beim Ändern einer Rolle. Dabei wird über den Button BERECHTIGUNGSDATEN ÄNDERN (siehe Abbildung 6.28) automatisch ein Abgleich der alten Profilwerte mit den aktuellen Vorschlagswerten der Vorschlagswerte für den Profilgenerator für die bereits vorhandenen und die neu hinzugefügten Transaktionen durchgeführt. Dabei werden alle Berechtigungsobjekte entzogen, die nicht dem aktuell über das Menü festgelegten transaktionalen Umfang der Rolle entsprechen, sofern die zugehörigen Berechtigungsobjekte im Profil nicht den Status *Manuell* oder *Geändert* aufweisen. Über den Button EXPERTENMODUS können Sie eine Pflegeart festlegen.

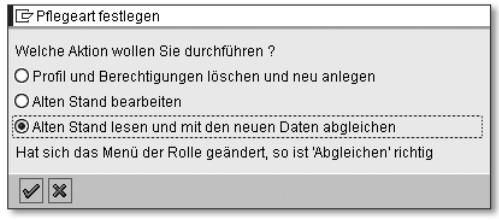


Abbildung 6.28 Profilgenerator, Registerkarte »Berechtigungen«: Expertenmodus zur Profilgenerierung

Die Funktion ALTEN STAND BEARBEITEN wird erfahrungsgemäß häufig verwendet, um den »erfahrungsfundierten« Zustand der Rolle nicht zu gefährden. »Erfahrungsfundiert« ist ein Euphemismus, den verschiedene Kunden benutzen: Er beschreibt den Sachverhalt, dass Rollen vielfach unter Außerachtlassung der Vorschlagswertpflege manuell geändert wurden. Wie in Abschnitt 7.1, »Pflege und Nutzung der Vorschläge für den Profilgenerator«, gezeigt wird, ist die einzige sinnvolle Form, Erfahrungen in die Definition von Rollen eingehen zu lassen, um die entsprechenden Vorschlagswerte zu pflegen. Die Funktion ALTEN STAND BEARBEITEN sichert letztlich nur den aktuellen Status der Rolle – und der ist oft genug mehr »Spontankorrektur«-getrieben als »erfahrungsbasiert«. Da Erfahrungsfundierung per se auf konzeptionellen Festlegungen und der Pflege der Vorschlagswerte basieren sollte, kann eine Pflege über diese Funktion nur ausnahmsweise sinnvoll sein.

Beim Anlegen und Ändern einer Rolle über ALTEN STAND LESEN UND MIT DEN NEUEN DATEN ABGLEICHEN wird erreicht, dass der transaktionale Umfang der Rolle mit den Vorschlägen für den Profilgenerator kombiniert einen Vorschlag für das Berechtigungsprofil der Rolle vorgibt. Abbildung 6.29 stellt die Übernahme der Vorschlagswerte dar.

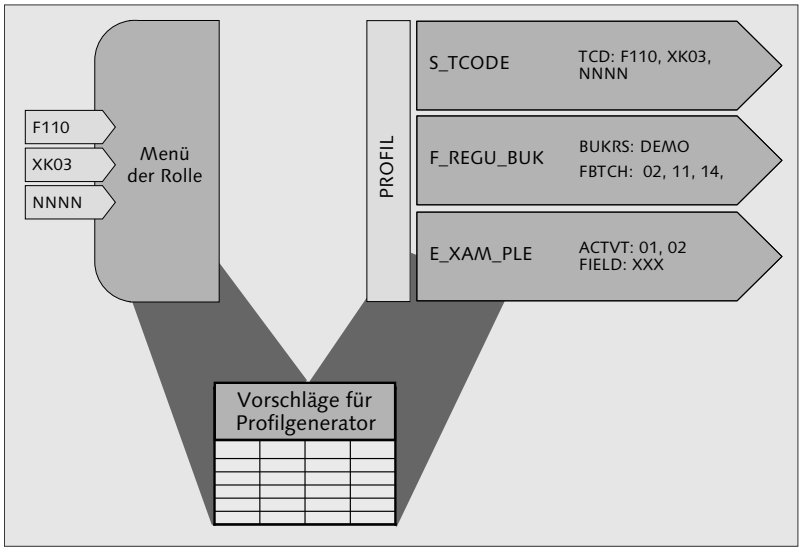


Abbildung 6.29 Übernahme der Vorschlagswerte für die im Menü vergebenen Transaktionen

Pflege der Organisationsebenen im Profilgenerator

Beim erstmaligen Aufruf des Profils erscheint der Bildschirm für die Eingabe von Organisationsebenen (siehe Abschnitt 3.7, »Organisationsebenen und -strukturen in SAP ERP«). Die Pflege der Organisationsebenen bewirkt, dass sämtliche Felder in Berechtigungsobjekten mit den an dieser Stelle vorgegebenen Werten gefüllt werden, es sei denn, diese sind auf Feldebene gepflegt.

Bei der Pflege im Berechtigungsfeld erscheint folgender Hinweis:

> *Die individuelle Pflege eines Orgebenenfeldes über das Dialogfenster* Feldwerte einpflegen *hat für dieses Feld in dieser Berechtigung folgende Konsequenzen: Die Wertepflege über das Dialogfenster* Orgebenen festlegen *verändert den Wert nicht mehr. Bei der Anpassung abgeleiteter Rollen wird der Berechtigungswert überschrieben. (Hinweis im Programm)*

Die individuelle Pflege von Organisationsebenen im Berechtigungsfeld ist meistens ein Hinweis auf Schwächen des betriebswirtschaftlichen Berechtigungskonzepts.

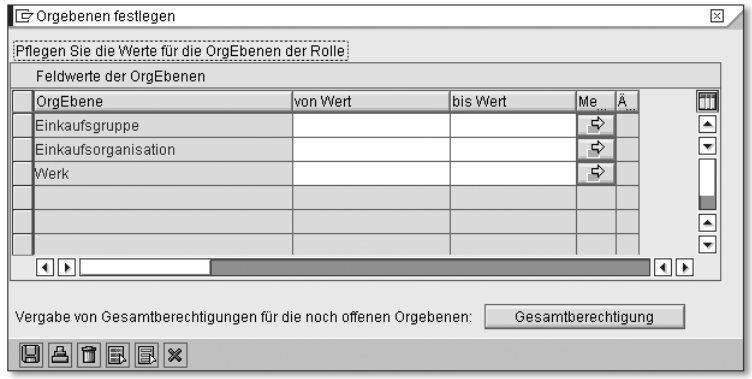


Abbildung 6.30 Profilgenerator, Registerkarte »Berechtigungen«: Organisationsebenen

Auf dem Bildschirm, der in Abbildung 6.30 gezeigt wird, werden die Organisationsebenen eingetragen. Sofern es sich um eine Vorlagerolle für abgeleitete Rollen handelt, empfiehlt es sich, die Werte maximal mit beliebigen, einheitlichen Buchstaben auszuprägen. Der Button Gesamtberechtigung ist vorhanden, um für offene Organisationsebenen die Gesamtberechtigung zu vergeben. Diese Option sollte nur dort genutzt werden, wo die Organisationsebenen tatsächlich nicht zur Differenzierung verwendet werden. Die Auswirkung

der korrekten Pflege der Organisationsebenen ist in Abbildung 6.31 dargestellt.

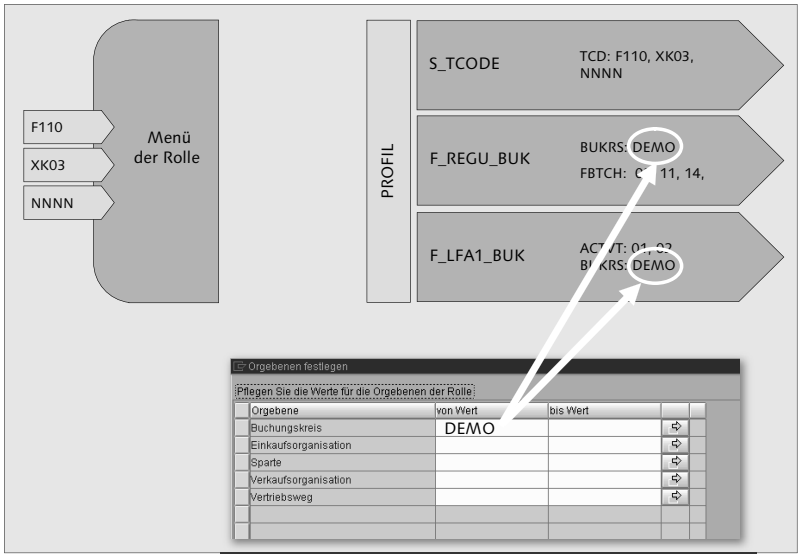


Abbildung 6.31 Übernahme der definierten Organisationsebene in die Rolle

Nach der Pflege der Organisationsebene kann das Profil Objekt für Objekt ausgeprägt werden.

Hinzufügen von Berechtigungsobjekten im Profil

Es besteht die Möglichkeit, auf verschiedenen Wegen Berechtigungsobjekte hinzuzufügen. Berechtigungsobjekte können über die Buttons Auswahl und Manuell in das Profil eingefügt werden. Das gewünschte Objekt kann entweder eingetragen oder über die Werthilfe selektiert werden (siehe Abbildung 6.32).

Abbildung 6.32 Profilgenerator, Registerkarte »Berechtigungen«: manuelles Einfügen von Berechtigungen

Zusätzlich können über Menü • Bearbeiten • Einfügen Berechtigungen Berechtigungen aus Profilen, Vorlagen oder Gesamtberechtigungen eingefügt werden (siehe Abbildung 6.33).

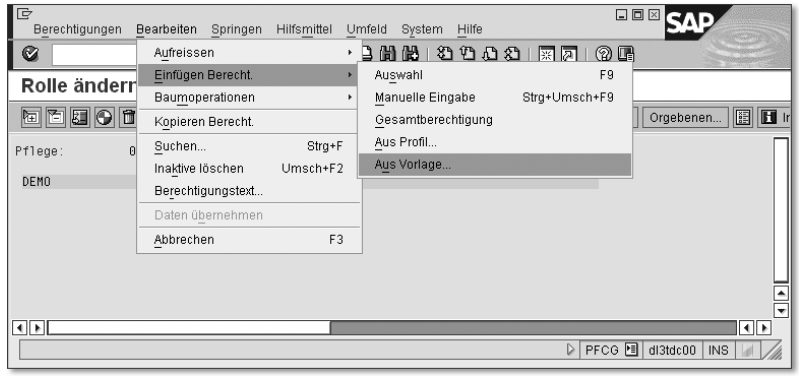


Abbildung 6.33 Profilgenerator, Registerkarte »Berechtigungen«: Einfügen von Berechtigungen aus Referenzen

In beiden Fällen werden die hinzugefügten Berechtigungsobjekte als manuell hinzugefügt gekennzeichnet (Status *Manuell*). Zwischen den in der Rolle enthaltenen Transaktionen und den Berechtigungsobjekten besteht somit kein nachvollziehbarer Zusammenhang, es sei denn, dass dieser Zusammenhang dokumentiert wird. Eine Möglichkeit der Dokumentation in der Rolle ist das jeweilige Berechtigungsobjekt selbst, dort kann das Feld Kurztext zur Berechtigung manuell ergänzt werden (siehe Abbildung 6.35, gekennzeichnet mit ❼).

Ausprägung von Berechtigungsobjekten im Profil

Nachdem im Profil die notwendigen Berechtigungsobjekte enthalten sind, müssen diese ausgeprägt und überprüft werden. Berechtigungsobjekte, die durch eine grüne Ampel und den Status *Standard* gekennzeichnet sind, entsprechen den Vorschlagswerten. Eine Überprüfung empfiehlt sich trotzdem, da viele SAP-Vorschlagswerte und ebenso die kundeneigenen nicht der gewünschten Funktion entsprechen müssen. Sofern eine Änderung erforderlich ist, müssen Sie den Vorschlagswert (Tabelle USOBT_C – Relation Transaktion → Ber.objekt (Kunde)) ändern. Insbesondere bei Enjoy-Transaktionen, die sowohl für die Pflege als auch die Anzeige genutzt werden sollen, kann es sinnvoll sein, den Vorschlagswert auf der Aktivität frei zu lassen (Berechtigungsobjekt wird dann ohne Ausprägung auf Aktivität vorgeschlagen). Die Änderung wird erst nach Pflege und Abgleich mit neuen Werten auf der Registerkarte Berechtigungen wirksam.

Prinzipiell haben Sie die Möglichkeit, jeweils durch Anklicken einer gelben Ampel für den untergeordneten Baumabschnitt Gesamtberechtigungen auf den offenen Feldern zu vergeben. Dies ist jedoch für Endbenutzerrollen im Produktivsystem niemals die Methode der Wahl. Die Ausprägung sollte immer konkret erfolgen, d. h., Sie sollten nur die Werte eintragen, die positiv benötigt werden. Um zu ermitteln, welche Werte wirklich benötigt werden, ist die Methode des Tracens (siehe Abschnitt 6.4, »Analyse von Berechtigungsprüfungen«) dringend zu empfehlen. Zusätzlich müssen Informationen vom Fachbereich über die Verwendung abgefragt werden. Letzteres gilt insbesondere für Werte, die sich nicht auf die Aktivität beziehen. Konkret werden im Trace zwar die Aktivität und z. B. eine Belegart abgebildet, regelmäßig kann es aber sein, dass mehrere Belegarten notwendig sind.

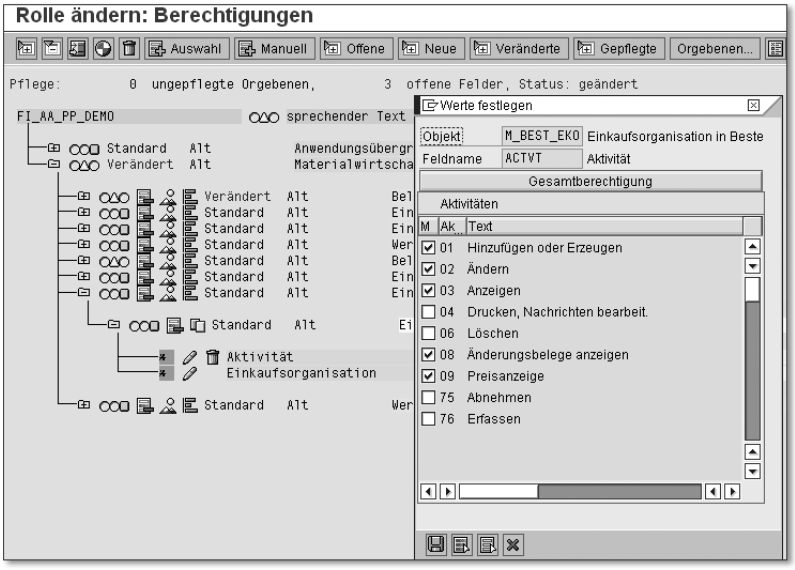


Abbildung 6.34 Profilgenerator, Registerkarte »Berechtigungen«: Profilpflege im Profilgenerator

Berechtigungsvorschläge, die teilredundant oder offensichtlich überflüssig sind, sollten nicht aus dem Profil gelöscht, sondern inaktiv gesetzt werden. Durch das Inaktivsetzen wird verhindert, dass derselbe Vorschlag beim nächsten Abgleichen über Alten Stand lesen und mit den neuen Daten abgleichen erneut eingefügt wird.

Die offenen Felder im Profil werden gepflegt. Es müssen nicht alle Felder gepflegt werden, vielmehr sollten nur die Felder gepflegt werden, deren Werte ermittelt wurden. Die gelbe Ampel und der Hinweis beim Generieren des Profils, dass nicht alle Objekte gepflegt wurden, bedeuten nicht unbedingt, dass die Berechtigungen unzureichend gepflegt wurden. Welche Felder eines Berechtigungsobjekts im Programmablauf geprüft werden, ist durch die Programmierung festgelegt. Es gibt Prüfungen, die nur ein Feld, aber nicht den Feldwert eines Berechtigungsobjekts prüfen, andere Prüfungen prüfen zwar die Aktivität als Feld, weitere Felder wie Berechtigungsgruppen werden aber nur dann geprüft, wenn diese Berechtigungsgruppe auch in den Daten des Geschäftsvorfalls auftaucht.

Generische Pflege eines Feldes

Berechtigungen können konkret, generisch und teilgenerisch gepflegt werden.

Feldausprägung	Art	Bedeutung
*	generisch	alle Werte
A*	teilgenerisch	alle Werte, die mit einem A anfangen
AAA	konkret	nur der Wert »AAA«
*A		nicht wirksam
A*A		nicht wirksam

Tabelle 6.1 Generische und konkrete Feldpflege

In Tabelle 6.1 sind in den ersten drei Zeilen die möglichen Ausprägungen dargestellt. Ein Stern bedeutet immer, dass alle Werte möglich sind. Dieser steht auch in Berechtigungsfeldern mit Vorschlagswerten zur Verfügung. Die teilgenerische Pflege ist nur mit dem Platzhalter Stern am Ende der Zeichenfolge möglich. Zur generischen Pflege beachten Sie auch SAP-Hinweis 1106948. Neben den dargestellten Möglichkeiten der Feldausprägung gibt es in einigen Fällen Platzhaltereinträge (siehe Tabelle 6.2).

Platzhalter	Beschreibung
''	Hochkomma, Hochkomma
' '	Hochkomma, Leerzeichen, Hochkomma
'	Hochkomma

Tabelle 6.2 Platzhalter

Ein Platzhalterzeichen muss dabei nicht immer als Platzhalter Verwendung finden, teilweise wird auch tatsächlich gegen das Platzhalterzeichen verprobt.

Exkurs: normativer Ansatz-Status von Berechtigungsobjekten

Berechtigungsobjekte können prinzipiell vier Status haben:

- Manuell – Das ganze Objekt wurde manuell hinzugefügt (❶ in Abbildung 6.35).
- Verändert – Der Vorschlagswert wurde verändert ❷.
- Gepflegt – Entspricht dem Vorschlagswert, es wurden Felder gepflegt ❸.
- Standard – Entspricht dem Vorschlagswert ❹.

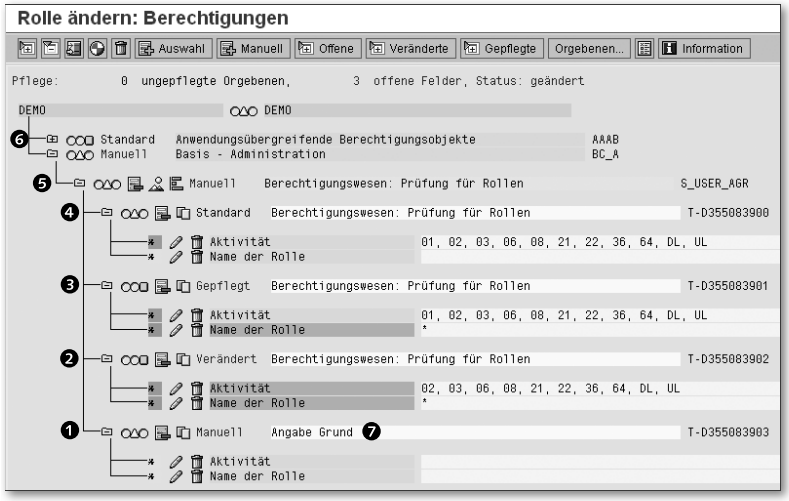


Abbildung 6.35 Status von Berechtigungsobjekten und Kurztext

Berechtigungsobjekte, die, wie im Abschnitt »Hinzufügen von Berechtigungsobjekten im Profil« beschrieben, hinzugefügt wurden, haben den Status *Manuell*. Berechtigungsobjekte, die über die Vorschlagswerte hinzugefügt wurden, können die Status *Standard*, *Gepflegt* und *Verändert* haben.

Die Ausprägung eines Objekts, die am weitesten von den Vorschlagswerten abweicht, kennzeichnet auch den Status des gesamten Berechtigungsobjekts ❺. Die weiteste Abweichung innerhalb einer Berechtigungsobjektklasse kennzeichnet den Status der Klasse ❻.

Eine Auswertung der Status und etwaiger Kurztexterläuterungen ist jederzeit über die Tabelle AGR_1250 (Berechtigungsdaten zur Aktivitätsgruppe) möglich (siehe Abbildung 6.36). Die mit ❶ gekennzeichnete Spalte enthält den Status des Berechtigungsobjekts (S – *Standard*, G – *Gepflegt*, M – *Verändert*, U – *Manuell*); die mit ❷ gekennzeichnete Zeile enthält den Kurztext zum Objekt, der manuell gepflegt werden kann.

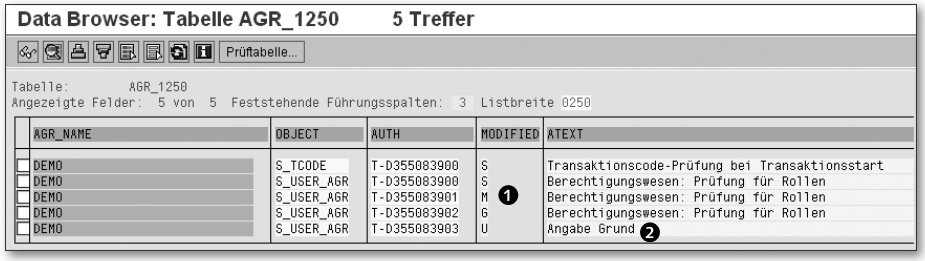


Abbildung 6.36 Tabelle AGR_1250 (Berechtigungsdaten zur Aktivitätsgruppe)

Maximal 10 % »Manuell« oder »Verändert«

In Abschnitt 7.1, »Pflege und Nutzung der Vorschläge für den Profilgenerator«, haben wir die Pflege von Vorschlagswerten und den Status von Berechtigungsobjekten diskutiert. An dieser Stelle soll schon das Ziel dargestellt werden, das es unserer Meinung nach zu erreichen gilt: Maximal 10 % der Status von Berechtigungsobjekten sollten *Manuell* oder *Verändert* sein. Abweichungen von den Vorschlagswerten sollten in einer Dokumentation auf Objektebene nachweisbar sein. Zu diesem Ansatz, der als »normativer Ansatz« bezeichnet werden kann, gibt im Sinne der Auditierbarkeit und der Upgrade-Sicherheit keine Alternative.

Profil generieren

Nach Ausprägung des Profils wird es generiert. Dadurch steht eine Rolle zur Verfügung, die den Benutzer mit einem Menü und detaillierten Berechtigungen versorgen kann, wie dies in Abbildung 6.37 dargestellt ist.

Registerkarte »Benutzer«

Auf der Registerkarte Benutzer kann die Zuordnung der Rolle zu einem Benutzer vorgenommen werden. Die technischen Möglichkeiten sind abhängig von den gewählten Einstellungen im Profilgenerator und der etwaigen Nutzung des Organisationsmanagements für die »indirekte Benutzerzuordnung», die in Kapitel 8, »Rollenzuordnung über das Organisationsmanagement«, behandelt wird.

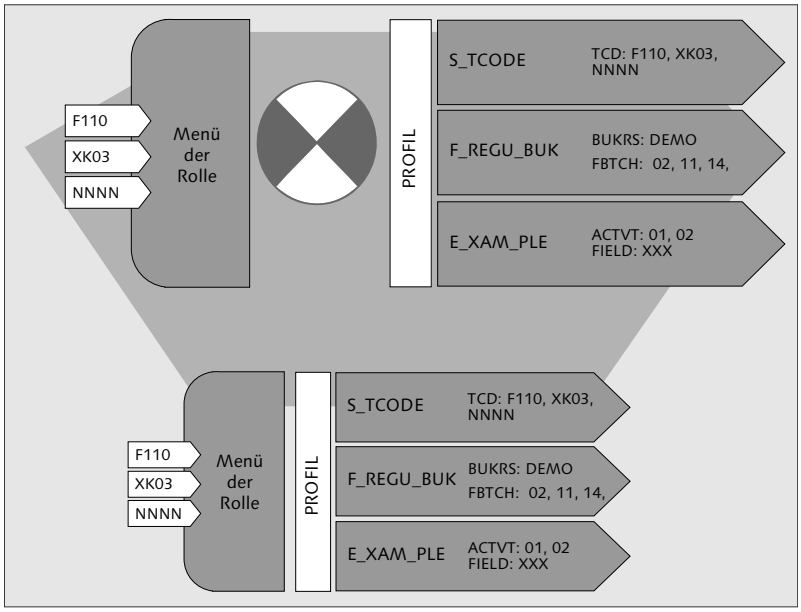


Abbildung 6.37 Generieren des Rollenprofils

Die Zuordnung einer Rolle zu einem Benutzer kann ebenfalls über die in Abbildung 6.38 dargestellte Pflege oder über die in Abbildung 6.6 gezeigte Pflege im Benutzerstammsatz erfolgen. Der Modus der Zuordnung ist weiterhin abhängig davon, ob (und wie) Access Control (siehe Kapitel 12, »SAP BusinessObjects Access Control«) und/oder die Zentrale Benutzerverwaltung und/oder das SAP NetWeaver Identity Management (siehe Kapitel 10, »Zentrales Management von Benutzern und Berechtigungen«) genutzt werden.

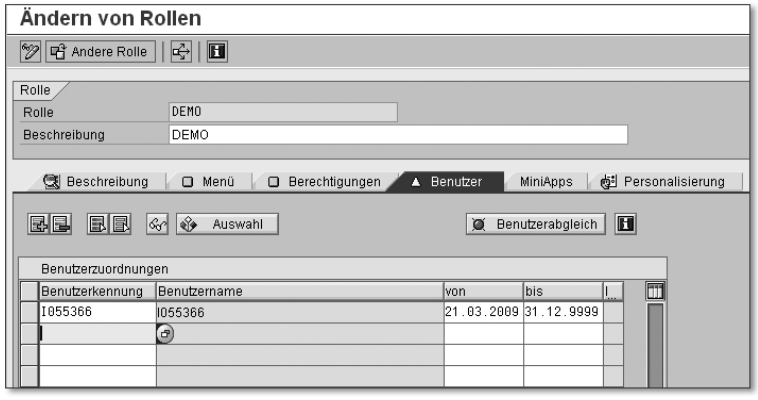


Abbildung 6.38 Registerkarte »Benutzerzuordnung«

Durch den Benutzerabgleich (Button Benutzerabgleich) werden die Berechtigungen der Rolle in den Benutzerpuffer des Benutzers eingetragen. Neben dem manuellen Benutzerabgleich steht per Voreinstellung in der Rollenpflege Menü • Hilfsmittel • Einstellungen der automatische Abgleich beim Speichern zur Verfügung.

Massenabgleich

Darüber hinaus stehen Massenabgleichsfunktionen über Reports (PFCG_TIME_DEPENDENCY und RHAUTUPD_NEW bzw. Transaktion PFUD (Abgleich Benutzerstamm)) zur Verfügung. SAP empfiehlt, den Report PFCG_TIME_DEPENDENCY als Hintergrundjob periodisch (möglichst täglich) einzuplanen, um einen regelmäßigen, vollständigen und zeitnahen Abgleich aller Benutzerstämme zu gewährleisten. Neue Berechtigungen werden hinzugefügt, alte entfernt. Nach dem Abgleich ist die ausgeprägte Rolle dem Benutzer zugeordnet, sodass ihm Menü und Berechtigungen wie definiert zur Verfügung stehen.

Registerkarte »Workflow«

Über die Registerkarte Workflow können einer Rolle Workflow-Aufgaben zugeordnet werden. Durch diese Zuordnung werden allerdings nicht die für die Erfüllung der Aufgabe notwendigen Berechtigungen zugeordnet, sondern die in der Rolle definierten. Dass die Zuordnung einer Workflow-Aufgabe Teil des Workflow-Konzepts ist, soll diese Möglichkeit in diesem Buch nicht vertieft werden.

Registerkarte »MiniApps«

MiniApps sind über den Web Application Builder erstellte Applikationen, die über einen Webbrowser (mySAP.com – Workplace) zur Verfügung gestellt werden und z. B. Reports über den Webbrowser zugänglich machen. Diese können auf der Registerkarte MiniApps zugeordnet werden. In einigen SAP-Standardrollen, unter anderem in den Rollen des Employee Self-Services, finden MiniApps Verwendung. Die Nutzung von MiniApps, die über Rollen bereitgestellt werden, erübrigt sich, sofern ein Portal im Einsatz ist.

Registerkarte »Personalisierung«

Die Funktion der Personalisierung dient dazu, der Anwendungsentwicklung ein Werkzeug zur »einfachen« Steuerung benutzerabhängiger Daten zu schaffen. Nach unserer Kenntnis gibt es aktuell wenige Beispiele für eine Verwendung dieser Funktionalität. Da die Personalisierung benutzerbezogen und rollenbezogen möglich wäre, kann gegebenenfalls festgelegt werden, woher die Daten übernommen werden sollen. Gegebenenfalls kann es zu konfliktären Angaben kommen. Tendenziell kann die Nutzung dieser Funktionalität zu einer Stei-

gerung der Komplexität führen. Detaillierte Angaben finden Sie in *Benutzer und Rollen (BC-SEC-USR)*, Release 6.20 (*http://help.sap.com/*).

Berichte über das Rollenmenü einbinden

Für den Fall, dass Berichte nicht bereits als Transaktion bereitstehen oder zu einer Transaktion eine zwingende rollenbezogene Variante vergeben werden soll, besteht die Möglichkeit, diese direkt in das Menü der Rolle einzubinden.

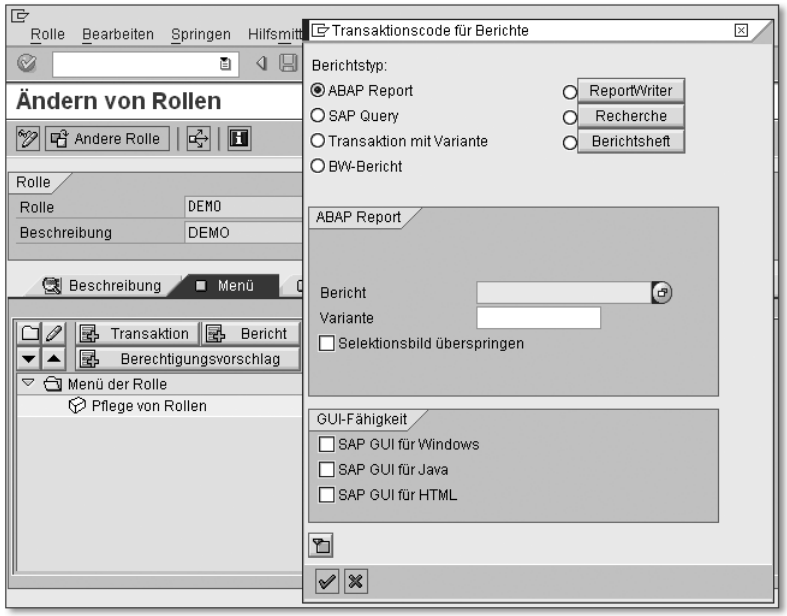


Abbildung 6.39 Zuordnung eines Berichts auf der Registerkarte »Menü«

Unterschiedliche Berichtsarten können auf diesem Wege eingebunden werden. In Abschnitt 7.6, »Parameter- und Query-Transaktionen«, wird beschrieben, wie eine Query unmittelbar in eine Transaktion umgesetzt werden kann. Aus diesem Grund erläutern wir Ihnen an dieser Stelle nur, wie ein Report-Writer-Bericht direkt in das Rollenmenü eingefügt werden kann.

Dazu klicken Sie auf den Button Report Writer (umfasst den auf Report Writer basierenden Report Painter ebenfalls). Im erscheinenden Auswahlbildschirm tragen Sie die Berichtsgruppe ein. Die Berichtsgruppe sollte durch die Fachseite genannt werden, im Zweifelsfall können Sie sie über die Transaktion GRR3 (Report Painter: Bericht anzeigen) ermitteln.

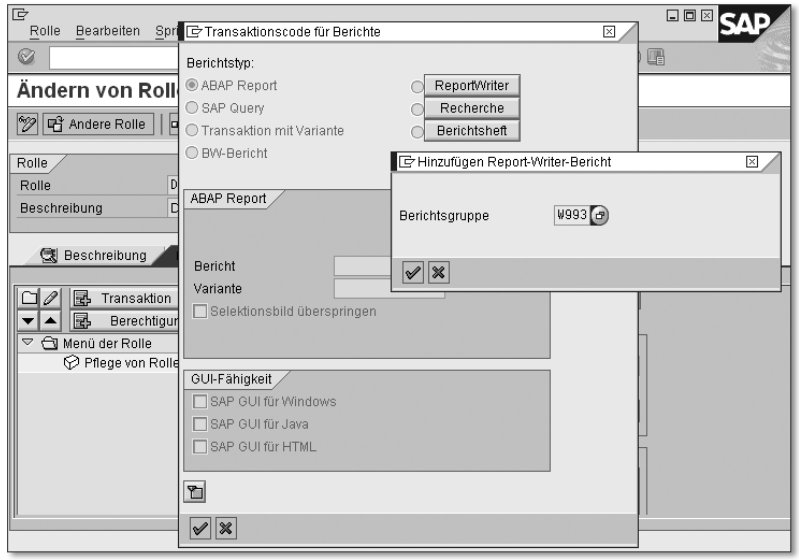


Abbildung 6.40 Auswahl Berichtsgruppe beim Einfügen eines Report-Writer-Berichts

Nach der Eingabe der Berichtsgruppe kann eine Selektionsvariante zu diesem Bericht (die bereits angelegt sein muss) mitgegeben werden. Dies ist vor allem dann interessant, wenn die Selektionsvariante als statische Einschränkung definiert ist – z. B., dass nur definierte Kostenarten angezeigt werden dürfen.

Die GUI-Fähigkeit muss definiert werden. Ebenso kann festgelegt werden, ob ein Transaktionscode automatisch generiert und ob die Beschreibung des Berichts übernommen werden soll. Sofern ein Transaktionscode generiert wird, muss dieser in einem Paket angelegt werden (zu Paketen siehe Keller/Krüger, 2006, S. 63–70).

Sofern bereits ein Transaktionscode existiert, wird dieser bei der Option AUTOMATISCH GENERIEREN übernommen. Bei der manuellen Pflege eines Transaktionscodes wird eine Warnmeldung ausgegeben, dass zu diesem Report bereits ein Transaktionscode existiert. Das Ergebnis ist eine ganz normale Transaktion im Menü.

Rollenableitung

Das Konzept der Rollenableitung basiert auf einem Konzept organisatorischer Differenzierung entlang der Organisationsebenen (siehe Kapitel 3, »Organisation und Berechtigungen«) im SAP-System. Die zugrunde liegende Idee ist, dass eine Rolle zunächst einmal eine Menge von funktionalen Zugriffen ist und diese funktionalen

Zugriffe in verschiedenen Organisationsteilen gleich sein werden. Sie müssen allerdings organisatorisch zu unterscheiden sein. Somit kann – rein logisch – eine Referenz angelegt werden, die jeweils organisatorisch differenziert wird.

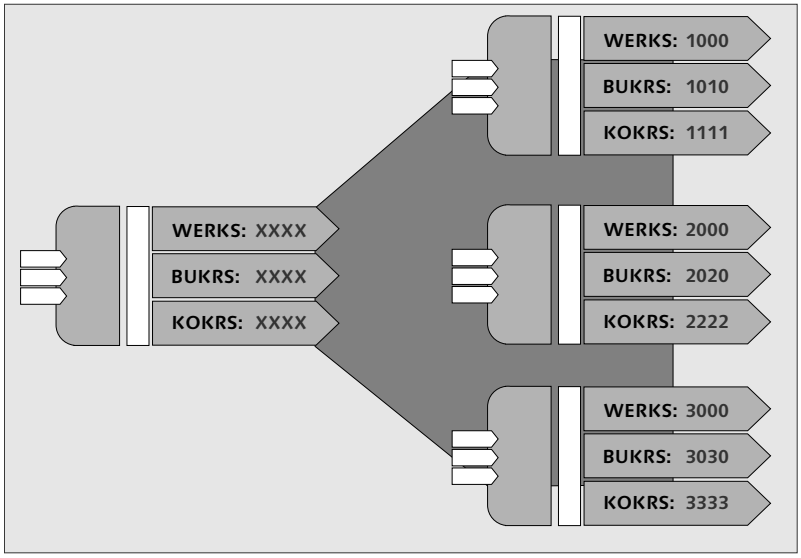


Abbildung 6.41 Referenzrolle – abgeleitete Rollen

Damit diese Differenzierung nicht dazu führt, dass eine logische Referenz 1.000-fach kopiert und individuell gepflegt wird, wird eine Ableitungsbeziehung hergestellt.

Referenzrolle

Eine logische Referenzrolle (entspricht der Vorlagerolle) für eine bestimmte Menge an Tätigkeiten wird so angelegt, dass die fachlichen Berechtigungen definiert sind. Die Ableitung erhält alle Berechtigungen und ermöglicht, diese Rolle für beliebig viele Organisationseinheiten auszuprägen, solange dies über die Organisationsebenen darstellbar ist. Das heißt, nur die Organisationsebenen sollen in den abgeleiteten Rollen unterschiedlich ausgeprägt werden.

Um eine Rolle abzuleiten, wird also eine Referenzrolle (entspricht einer Vorlagerolle) benötigt. Aus Gründen der Übersichtlichkeit raten wir Ihnen dringend, diese Referenzrolle keinem Benutzer zuzuordnen und fiktiv auszuprägen. Fiktiv ausprägen bedeutet in diesem Fall, dass alle tatsächlich zur Differenzierung genutzten Organisationsebenen in der Referenzrolle mit fiktiven Werten ausgeprägt wer-

den (siehe Abbildung 6.42). Die Referenzrolle sollte laut Namenskonzept auch eindeutig identifizierbar sein.

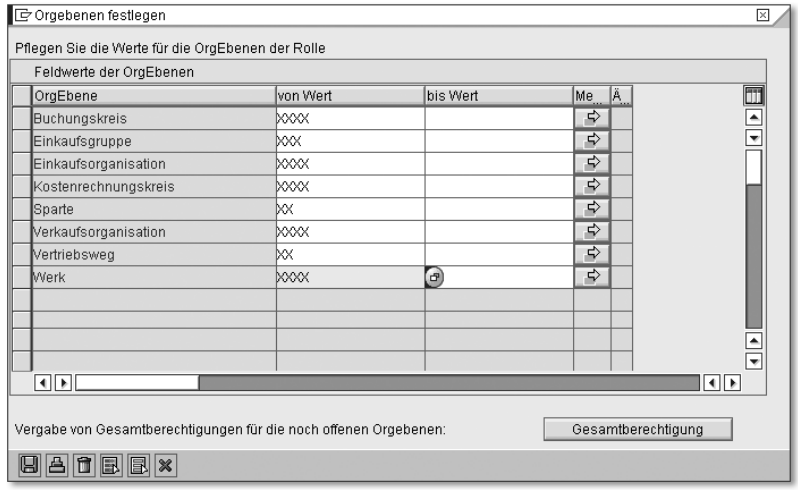


Abbildung 6.42 Fiktive Ausprägung der Organisationsebenen einer Referenzrolle

Der Feldwertpflege in der Referenzrolle kommt im Rahmen des Ableitungskonzepts eine besondere Bedeutung zu. Diese Werte definieren die Berechtigungen für alle abgeleiteten Rollen. Das bedeutet auch, dass eine auf Feldebene gepflegte Organisationsebene genau so in der abgeleiteten Rolle im entsprechenden Feld vorhanden sein wird.

Ableitung

Bei der Ableitung wird auf die Referenzrolle Bezug genommen. Dieser Bezug ist einerseits, wie dargestellt wird, ein technischer Bezug, andererseits ist es auch ein betriebswirtschaftlicher Bezug. Die Referenzrolle ist faktisch eine normative Vorgabe von Berechtigungen über die Grenzen von Organisationseinheiten hinweg. Auch abgeleitete Rollen sollten im Rahmen der geltenden Namenskonvention eindeutig identifizierbar sein.

Das Ableiten einer Rolle ist nur (einmalig) beim Anlegen möglich. Bevor die Rolle erstmalig gespeichert wird, muss die Ableitungsbeziehung durch Eintrag in das Feld Ableiten aus Rolle definiert sein. Beim Sichern der Rolle erfolgt dann eine Sicherheitsabfrage, ob die Referenzrolle wirklich als vererbende Rolle eingetragen werden soll. Sobald die Rolle gesichert ist, kann die Ableitungsbeziehung nicht mehr geändert, sondern nur noch ersatzlos aufgelöst werden.

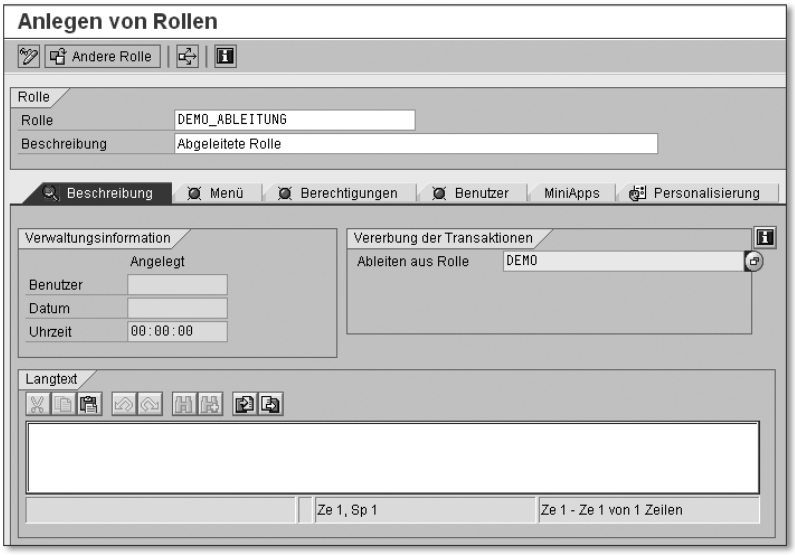


Abbildung 6.43 Ableiten beim Anlegen einer Rolle

Nachdem die Ableitungsbeziehung definiert (und das Menü automatisch übernommen) wurde, ist eine Pflege des Menüs nicht mehr zulässig. Dies ergibt sich systematisch aus dem Ableitungskonzept, funktionale Änderungen und damit auch das Hinzufügen von Transaktionen verstoßen gegen das Konzept. Sie stellen ein logisches Abweichen von der durch eine funktional definierte Referenzrolle und eine rein organisatorisch differenzierende Ableitung in die abgeleitete Rolle dar.

Die abgeleitete Rolle wird also nur im Profil gepflegt. Dabei werden zunächst die Organisationsebenen abgefragt. Nach der Pflege der Organisationsebenen stellt sich die Rolle wie in Abbildung 6.44 dargestellt dar, d. h., der Zustand der Berechtigungsobjekte entspricht den Vorschlägen der Vorschlagstabelle. Über den Button Daten übernehmen (in der Abbildung mit ❶ gekennzeichnet) werden alle Werte der Referenzrolle mit Ausnahme der in der Ableitung bereits gepflegten Organisationsebenen übernommen.

Der Datenübernahme in der abgeleiteten Rolle entspricht in der Referenzrolle der Button Abgeleitete Rollen generieren, der allerdings zusätzlich noch das Profil der abgeleiteten Rollen generiert. Beide Buttons gleichen alle Werte mit Ausnahme der Organisationsebenen ab.

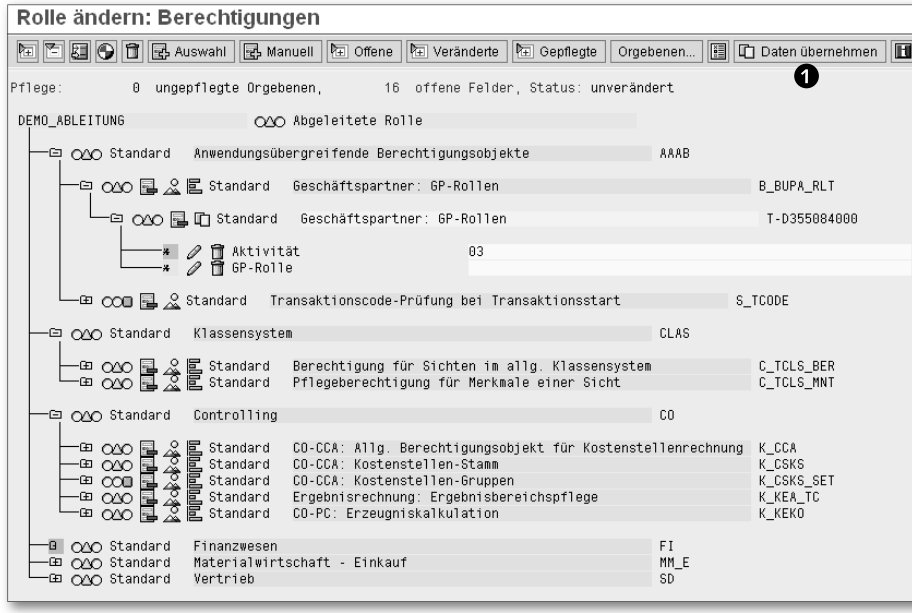


Abbildung 6.44 Abgeleitete Rolle/Datenübernahme

Die Navigation zwischen Referenzrolle und abgeleiteter Rolle wird erheblich durch die Vererbungshierarchie erleichtert. Der durch ❶ in Abbildung 6.45 gekennzeichnete Button öffnet die Vererbungshierarchie, in der durch Klicken zwischen den Rollen navigiert werden kann. Die Ableitungsbeziehung ist mit ❷ gekennzeichnet. Die Vererbung kann auch gut über die Tabelle AGR_DEFINE (Definition Rollen) ausgewertet werden.

Anmerkung zum Ableitungskonzept

In Reviews ist häufig festzustellen, dass das Ableitungskonzept nicht stringent umgesetzt wird.

Beispiel

Ein extremes Beispiel ist der Konzern, bei dem in Bezug auf 100 Referenzrollen und 7.000 Ableitungen mehr als 260.000 Abweichungen nachgewiesen werden konnten. In diesem Fall bestand das Ableitungskonzept nur noch nominell, faktisch war es so weit degeneriert, dass es weder betriebswirtschaftlich noch technisch sinnvoll war.

Gründe für Abweichungen

Zu diesen Abweichungen kann es kommen, wenn die Rollen nicht regelmäßig abgeglichen werden (über die Funktion im Profil der

Referenzrolle *Abgeleitete Rollen generieren* oder in der abgeleiteten Rolle *Daten übernehmen*).

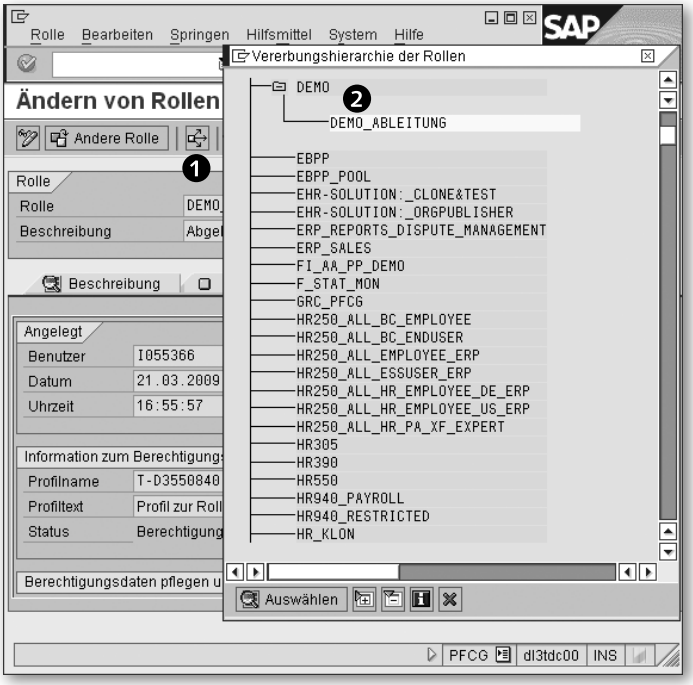


Abbildung 6.45 Vererbungshierarchie der Rollen

Die Arten, wie die abgeleitete Rolle degeneriert, sind mannigfaltig. Üblich sind manuelle Ergänzungen von Werten, aber auch manuelles Pflegen von Organisationsebenen im Objekt konnte nachgewiesen werden. Da diese Änderungen willentlich durchgeführt wurden, ist dieses Vorgehen ein bewusstes Umgehen des Ableitungskonzepts. Somit entsteht in jedem Fall eine Sicherheitslücke – vorausgesetzt, das Ableitungskonzept wird normativ begriffen – und eine zusätzliche Steigerung der Komplexität. Das Außerkraftsetzen eines technischen Standards muss in der täglichen Wartung berücksichtigt werden und steigert die Kosten jedes Upgrade-Projekts um die Anzahl der degenerierten Rollen. Die Firma, die im gegebenen Beispiel für die operative Pflege verantwortlich war, bezifferte den Aufwand für die Überführung während des Upgrades mit mehreren hundert Personentagen.

Berechtigungsvorlagen

Berechtigungsvorlagen sind systematisch vordefinierte Rollenprofile, die in der Profilpflege in eine Rolle übernommen werden können. SAP liefert standardmäßig einige dieser Vorlagen aus, es können weitere kundeneigene Vorlagen verwendet werden.

Vorlagen in Profile einfügen

Zur Übernahme der Vorlage in ein Profil haben Sie zwei Möglichkeiten:

- Sofern die Rolle keine Transaktionen und Berechtigungsobjekte enthält, werden standardmäßig die Vorlagen angeboten.
- Sofern bereits Berechtigungsdaten vorhanden sind oder aus dem Menü vorgeschlagen werden, kann über den Pfad • BEARBEITEN • EINFÜGEN BERECHTIGUNGEN • AUS VORLAGE der Vorlagedialog aufgerufen werden.

Die Nutzung von Vorlagen führt einerseits dazu, dass die so übernommenen Berechtigungsobjekte in der Rolle mit dem Status *Manuell* ausgewiesen werden und dass die Übernahme des Objekts aus einer Vorlage nicht als solche dokumentiert und somit nicht nachvollziehbar ist.

Die Nutzung führt aber auch – anders als ein Modell mit Ableitungen – dazu, dass eine Änderung der Vorlage nicht wirksam für die vormals darauf basierenden Rollen ist.

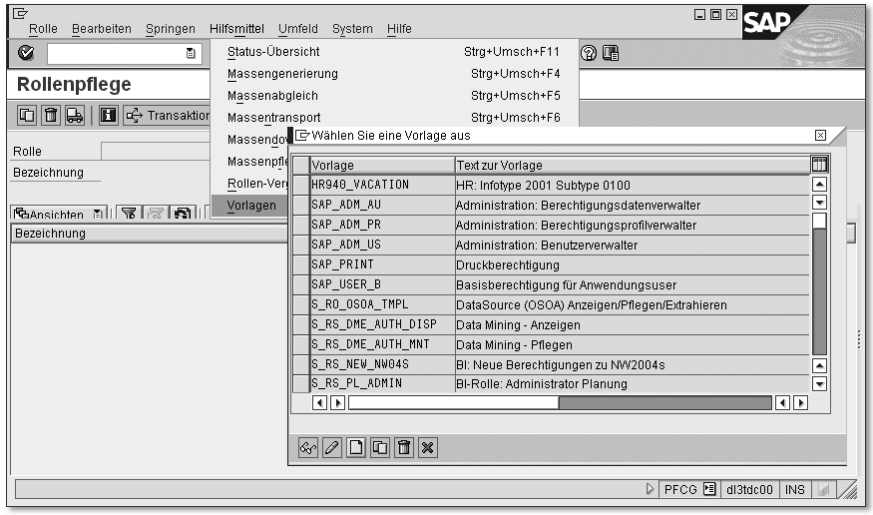


Abbildung 6.46 Einstieg in die Pflege von Vorlagen im Profilgenerator

Vorlagen pflegen

Berechtigungsvorlagen können in kundeneigene Vorlagen kopiert oder gänzlich durch den Kunden selbst angelegt werden (siehe Abbil-

dung 6.47). Der Namensraum ist nur beschränkt darauf, dass kein S als Präfix genutzt wird.

Dazu stehen in der Pflege der Transaktion SU24 (Vorschlagswerte für den Profilgenerator) und im Profilgenerator über die Transaktion PFCG (Pflege von Rollen) selbst zwei Wege zur Verfügung. Im Profilgenerator werden die Vorlagen über HILFSMITTEL • VORLAGEN gepflegt.

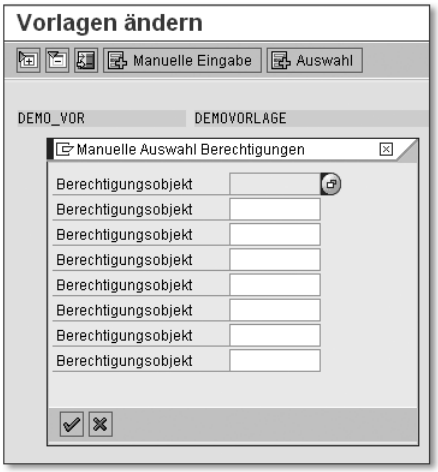


Abbildung 6.47 Berechtigungsvorlage pflegen

Wie im Profilgenerator können Objekte auf verschiedenen Wegen hinzugefügt werden. Beim Speichern muss die Vorlage entweder als lokales Objekt übernommen oder als Objektkatalogeintrag hinterlegt werden (das Vorgehen wird unter *http://help.sap.com/* im *BC – Change and Transport Organizer* beschrieben).

6.4 Analyse von Berechtigungsprüfungen

Eine der bereits formulierten Anforderungen an die Pflege von Berechtigungen ist die, dass nur Berechtigungswerte vergeben werden, die eindeutig notwendig für die Ausführung einer bestimmten und legitimen Aktion sind.

Wie bereits angesprochen, ist eine erforderliche Quelle für diese Werte die Vorschlagstabelle, die in Kapitel 7, »Systemeinstellungen und Customizing«, ausführlicher dargestellt werden soll. Diese kann

allerdings selbst bei ausführlicher Pflege nicht alle Werte enthalten. Dazu ein Beispiel: Eine Organisation möchte Berechtigungen über die Belegart in der Bestellung differenzieren, also kann als Vorschlagswert auf der Bestellung nicht die Belegart konkret mitgegeben werden.

Neben der Analyse der Vorschlagswerte gibt es noch drei weitere Wege, um zu ermitteln, welche Berechtigungen benötigt werden:

- die Fehlerprüfung (Auswertung der Berechtigungsprüfung)
- den Berechtigungstrace
- die Prüfung des Programms

Diese werden wir im Folgenden betrachten.

6.4.1 Auswertung der Berechtigungsprüfung

Die Transaktion SU53 (Auswertung der Berechtigungsprüfung) ist mit Sicherheit die ineffizienteste Methode. Ausgewertet wird, möglichst durch den Benutzer selbst, welche Berechtigungen für einen Schritt erforderlich gewesen wären. Dazu führt der Benutzer, nachdem die Ausführung wegen mangelnder Berechtigungen abgebrochen wurde, die Transaktion aus und stellt die Auswertung gegebenenfalls über einen Screenshot zur Verfügung. In Abbildung 6.48 ist der Bereich umrandet, der Details zu der fehlenden Berechtigung enthält.

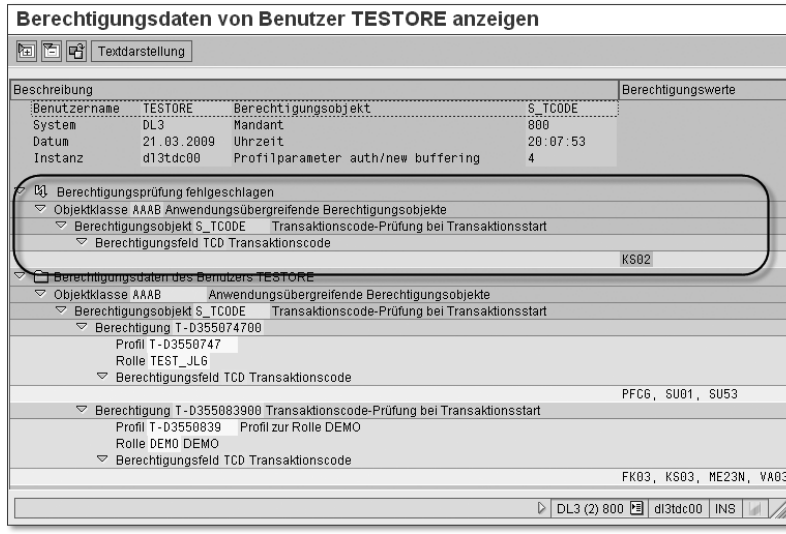


Abbildung 6.48 Auswertung der Berechtigungsprüfung

Reine Fehlerprüfung

Dieses Vorgehen ist deshalb ineffizient, weil nur der aktuelle Fehler ermittelt wird. In der vereinfachten Darstellung in Abbildung 6.11 sind bereits fünf Prüfungen von Berechtigungsobjekten im Programmablauf dargestellt. In diesem Beispiel müsste also ein Benutzer fünfmal den Fehler über die Transaktion SU53 (Auswertung der Berechtigungsprüfung) ermitteln und mitteilen. Diese Methode ist nichts anderes als eine Fehlerprüfung – es wird immer die letzte fehlgeschlagene Berechtigungsprüfung angelegt. Sie weist aber nicht eventuell zu umfassende Berechtigungen aus, und sie weist auch nicht aus, welche weiteren Berechtigungen im Programmablauf noch fehlen werden.

Entsprechend ist die Methode nur für den Support produktiver Rollen in einem eingeführten und umgesetzten Berechtigungskonzept sinnvoll. Mit dieser Methode neue Rollen anlegen zu wollen führt zu einem nicht akzeptablen Aufwand.

6.4.2 Analyse im Programmablauf System-Trace/Berechtigungstrace

Es gibt zwei Arten, Berechtigungen zu tracen, d. h. aufzuzeichnen, welche Berechtigungen im Programmablauf tatsächlich überprüft werden. Die eine Art ist der im Folgenden dargestellte System-Trace, die andere wird in Abschnitt 7.8, »Entwickler- und Berechtigungstrace«, erläutert.

Der System-Trace wird in der fallbezogenen Ermittlung von Berechtigungen eingesetzt. Der Entwickler-Trace wird vor allem für kundeneigene Transaktionen, die keine Einträge in der Vorschlagswerttabelle USOBT (Relation Transaktion → Ber.Objekt) haben, genutzt. Der Entwickler-Trace gehört zur Entwicklung und Dokumentation von Programmen.

Der Trace, Transaktion ST01 (System-Trace), sollte eingeschränkt werden auf den Gegenstand der Analyse, d. h., regelmäßig ist die Berechtigungsprüfung (einschränken über Trace-Komponenten im Einstiegsbildschirm) nur für einen Benutzer oder eine Transaktion von Interesse. Benutzer oder Transaktion werden entweder über den Button Allgemeine Filter oder über den in Abbildung 6.49 dargestellten Menüpfad eingeschränkt.

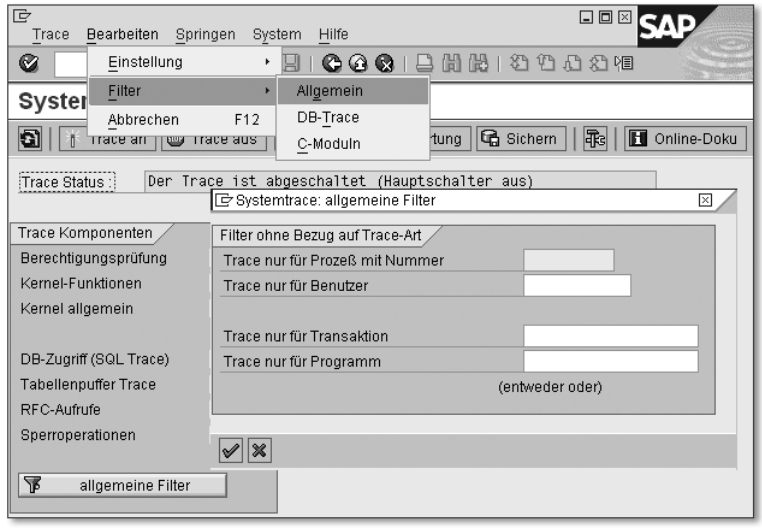


Abbildung 6.49 System-Trace: Einstiegsbildschirm

Der gewählte Benutzer kann (in einem Testsystem) ein Benutzer mit sehr umfangreichen Berechtigungen sein. Nach der einschlägigen Einschränkung des Traces auf den notwendigen Analyserahmen wird der Trace aktiviert. Nach dem Einschalten des Traces kann mit der Aufzeichnung begonnen werden.

Experten-unterstützung

Aufgezeichnet wird die fachlich korrekte Ausführung einer Transaktion, z. B. das Anlegen einer Bestellung. Erfahrungsgemäß sollte die Transaktion im gewünschten prozessualen Umfang durch einen Experten des jeweiligen Fachbereichs durchgeführt werden. Diesem und nur diesem sind nämlich auch gewünschte Einschränkungen im funktionalen oder organisatorischen Umfang der Ausführung bekannt. Er ist es auch, der die impliziten und jeweils gewünschten organisationsspezifischen Einschränkungen kennt.

Um die Experten nicht zeitlich zu sehr zu binden, lohnt es sich, auch ganze Rollen oder sogar noch mehr aufzuzeichnen. Das erfordert dann allerdings etwas mehr Aufwand in der Auswertung.

Die Auswertung des Traces wird über den Button Auswertung erreicht. Sofern vorab keine Einschränkung vorgenommen wurde, kann an dieser Stelle noch eine Selektion die Treffermenge auf ein sinnvolles Maß beschränken.

Abbildung 6.50 System-Trace: Auswertung

Die Anzeige des Traces ermöglicht eine zügige Erfassung der überprüften Berechtigungsobjekte. Sofern es um einen Trace geht, der eine große Menge von Prüfungen enthält, empfiehlt es sich dringend, den Trace in ein Format zu übertragen, das einschlägige Auswertungen und Gruppierungen ermöglicht.

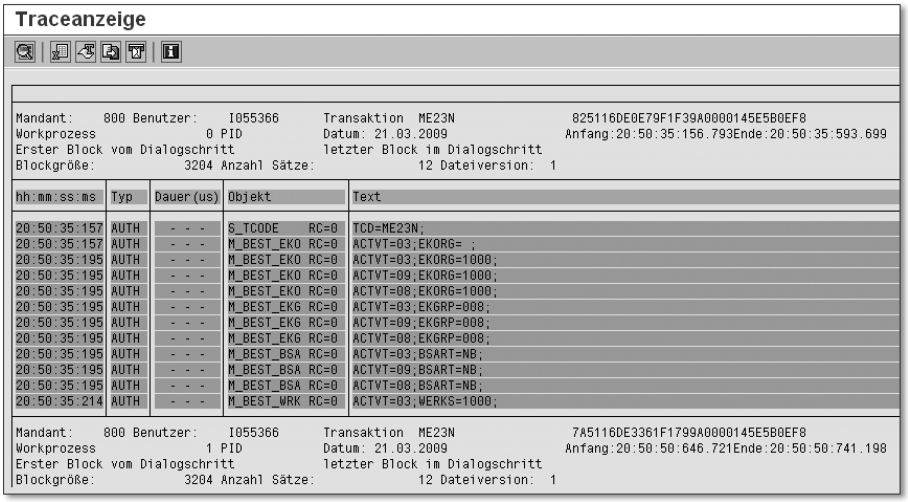


Abbildung 6.51 System-Trace: Anzeige

Gehen Sie bei der Interpretation der Werte vorsichtig vor, der Trace kann Werte enthalten, die durch das erstmalige Ausführen der Transaktion benötigt werden. Er wird mit Sicherheit auch Werte enthalten,

die durch allgemeine Endnutzerrollen wie die sogenannten *unkritischen Basisberechtigungen* vergeben werden.

Beachten Sie darüber hinaus, dass der Absprung in eine andere Transaktion im Trace dadurch nachzuvollziehen ist, dass diese Transaktion aufgezeichnet wurde, die im Trace folgenden Werte beziehen sich somit auf die Transaktion, auf die abgesprungen wurde.

6.4.3 Prüfung des Programms

Prinzipiell stehen mehrere Möglichkeiten zur Verfügung, um die Berechtigungsprüfungen in Programmen, Includes etc. nachzuweisen:

In der Transaktion SE80 (Object Navigator) können Sie im Programm den String `authority-check` suchen (siehe Abbildung 6.52).

Über den Report RPR_ABAP_SOURCE_SCAN (ABAP Source Scan) können Sie ebenfalls im benannten Programm den String `authority-check` suchen.

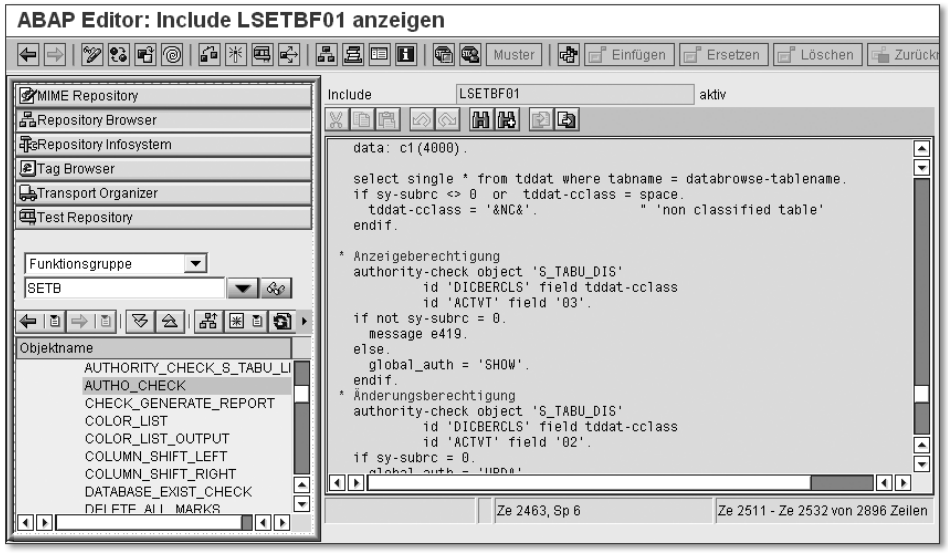


Abbildung 6.52 String »authority_check« im Programm SETB

Schließlich kann in den Verwendungsnachweisen überprüft werden, wo ein bestimmtes Berechtigungsobjekt Verwendung gefunden hat. Im Beispiel, das in Abbildung 6.53 dargestellt ist, wird der Verwen-

dungsnachweis über die Transaktion S_BCE_68001413 (Berechtigungsobjekte nach komplexen Selektionskriterien) ausgeführt. Dazu klicken Sie auf den Button VERWENDUNGSNACHWEIS, der in Abbildung 6.53 markiert ist.

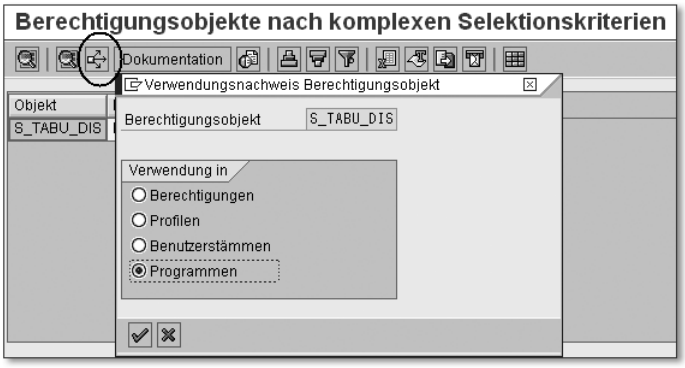


Abbildung 6.53 Verwendungsnachweis von Berechtigungsobjekten

Nach einem weiteren Selektionsschritt, in dem in diesem Beispiel auf Transaktionen und Programme eingeschränkt wurde, wird der in Abbildung 6.54 dargestellte Verwendungsnachweis ausgegeben.

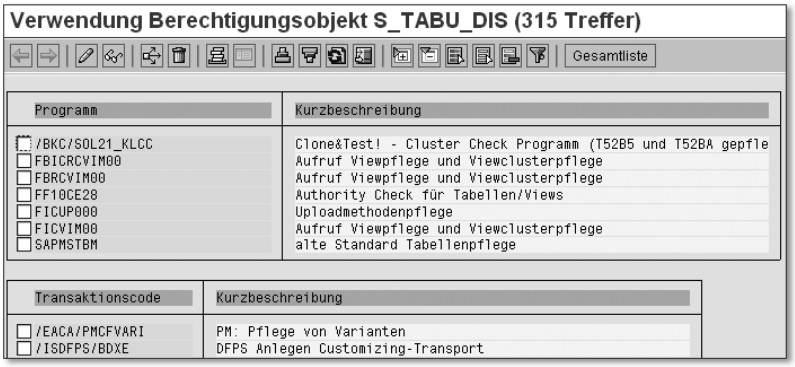


Abbildung 6.54 Verwendungsnachweis

6.5 Weitere Rollentypen in SAP ERP

Neben der bisher besprochenen Rolle, im Sinne einer Einzelrolle, und der abgeleiteten Rolle (die immer auch eine Einzelrolle ist) stehen im Standard noch die Sammelrolle und die Rollenmanager-Rolle zur Verfügung. Da die Rollenmanager-Rolle ein unbekannter Typ ist

und eines weiteren umzusetzenden technischen Konzepts bedarf, soll diese in Kapitel 9, »Automatisierte organisatorische Differenzierung: der Rollenmanager«, besprochen werden.

Ergänzend zum Standard gibt es noch konzeptionelle Differenzierungsmöglichkeiten, die teilweise werkzeugabhängig sind. Als Typisierung bietet sich die in Tabelle 6.3 dargestellte Unterscheidung an.

Rollentyp	Differenzierung	Erklärung
Einzelrolle	Einzelrolle	Standard: Einzelrolle zur direkten Verwendung
	Referenzrolle/ Vorlagerolle	Einzelrolle, die lediglich als Referenz zum Ableiten dient
	abgeleitete Rolle	Einzelrolle, die aus einer Vorlagerolle abgeleitet wurde
	Rollenmanager-Rolle	Einzelrolle, die durch den ABAP-Rollenmanager erzeugt und zugewiesen wird
	Wertrolle	Einzelrolle, die ausschließlich Berechtigungsobjekte zur organisatorischen Differenzierung nutzt
	funktionale Rolle	Einzelrolle. Logisches Pendant zur Wertrolle, in der funktionalen Rolle sind alle erforderlichen Berechtigungen enthalten, mit Ausnahme der Berechtigungsobjekte zur organisatorischen Differenzierung.
Sammelrolle		Kombination von Einzelrollen
Enterprise-Rolle (Access Control)		Kombination verschiedener Rollen, sowohl Einzel- als auch Sammelrollen, gegebenenfalls systemübergreifend

Tabelle 6.3 Rollentypisierung

6.5.1 Sammelrolle

Die Sammelrolle ist die Kombination beliebig vieler Einzelrollen, wenn gewünscht, unter Zusammenstellung eines integrierten Sammelrollenmenüs. Die Sammelrolle wird auch über den Profilgenerator über die Transaktion PFCG (Pflege von Rollen) angelegt, im Einstiegsbildschirm klicken Sie dazu auf den Button Sammelrolle

ANLEGEN. Die erste Registerkarte BESCHREIBUNG muss sinngemäß wie bei einer Einzelrolle gepflegt werden. Auf der zweiten Registerkarte ROLLEN können nun die gewünschten Rollen hinzugefügt werden. Auf der dritten Registerkarte MENÜ kann das Menü der Einzelrollen eingelesen und durch weitere Buttons bereinigt/integriert werden.

Die Sammelrolle ist funktional die Bündelung von Einzelrollen, um gegebenenfalls einen Aufgabenzusammenhang oder unter Umständen einen Stellenzusammenhang abbilden zu können (siehe Abbildung 6.55). Diese Bündelung ist dort sehr sinnvoll einzusetzen, wo Teilaufgaben unterschiedlichen Aufgaben oder Aufgaben unterschiedlichen Stellen zugeordnet werden können (siehe Kapitel 3, »Organisation und Berechtigungen«).

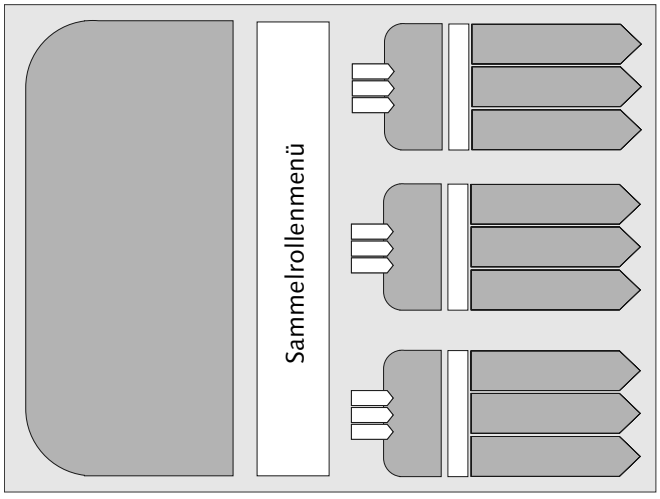


Abbildung 6.55 Sammelrolle

6.5.2 Wertrolle/funktionale Rolle

Einige Berechtigungskonzepte differenzieren zwischen *Wertrollen* und *funktionalen Rollen*. Dies ergibt sich teilweise aus dem Einsatz eines entsprechenden Werkzeugs, es kann aber auch rein konzeptionelle Gründe dafür geben.

Eine funktionale Rolle in diesen Konzepten ist eine Rolle, die alle gewünschten Berechtigungen enthält, nur die Berechtigungsobjekte nicht, die Felder enthalten, die zur organisatorischen Differenzierung genutzt werden. Dabei ist es unerheblich, ob die Felder als Organisa-

tionsebenen angelegt oder einfache Felder sind. Diese Berechtigungsobjekte werden in eigenen Rollen, den Wertrollen, zusammengefasst.

Erst die Kombination von beiden Rollentypen im Benutzerpuffer soll die tatsächlichen Berechtigungen darstellen.

Die Art der Zusammenfassung kann sehr unterschiedlich sein. So sind uns Wertrollenkonzepte begegnet, in denen schlicht alle organisatorisch unterscheidenden Berechtigungsobjekte zusammengefasst waren und alle Aktivitäten berechtigt waren. Diese Herangehensweise ist gleich doppelt falsch, einerseits gibt es so gut wie keine Organisation, in der Organisationsteile durch eine übergreifende Sammlung berechtigt werden können. Andererseits ist natürlich die Berechtigung für alle Aktivitäten niemals angemessen, sie würde voraussetzen, dass die funktionalen Rollen des Benutzers ausschließlich die Differenzierung auf Aktivitäten leisten. Das ist so aber einfach nicht möglich. Wertrollenkonzepte sind nur dort sinnvoll, wo eine kleine Gruppierung organisatorischer Merkmale zusammengefasst wird und zusätzlich auch in den Aktivitäten unterschieden wird. So kann es durchaus sinnvoll sein, die Kostenstellenberechtigungen (Feld KOSTL sowie RESPAREA) zusammenzufassen und zusätzlich minimal zwischen den Aktivitäten Anlegen, Buchen und Anzeigen zu unterscheiden.

6.6 Fazit

In diesem Kapitel haben Sie, ausgehend vom Benutzer, erfahren:

- wie der Benutzer gepflegt wird
- worin der Zusammenhang zwischen Transaktion, Programm und Berechtigungsobjekt besteht
- wie Sie Rollen pflegen
- welche Standards Sie bei der Rollenpflege einhalten sollten
- wie Sie Berechtigungsprüfungen analysieren können
- welche weiteren Rollentypen es gibt

Durch die zahlreichen Verweise auf spätere Kapitel sollte auch deutlich werden, dass die Berechtigungspflege weit mehr umfasst als die bloße Definition einer Rolle.

Die organisatorische Differenzierung ist die größte Herausforderung für ein Rollenkonzept. Der Rollenmanager ermöglicht eine weitgehende, sehr effiziente und präzise Automatisierung. Die möglichen Konzepte werden in diesem Kapitel entwickelt.

9 Automatisierte organisatorische Differenzierung: der Rollenmanager

In Kapitel 3, »Organisation und Berechtigungen«, haben wir erläutert, dass organisatorische Differenzierung eine wesentliche und komplexe Anforderung an das betriebswirtschaftliche Berechtigungskonzept stellt. In Kapitel 6, »Technische Grundlagen der Berechtigungspflege«, haben wir das Ableitungskonzept und in Kapitel 8, »Rollenzuordnung über das Organisationsmanagement«, die indirekte Rollenzuordnung vorgestellt. Diese Konzepte dienen der organisatorischen Differenzierung und der Zuordnung organisatorisch differenzierter Rollen.

Umfassende organisatorische Differenzierung führt zu einem exponentiellen Wachstum der Anzahl abgeleiteter Rollen. Dieser Aufwand lässt sich durch die Nutzung des Rollenmanagers erheblich reduzieren. In diesem Kapitel stellen wir den Rollenmanager dar, der die organisatorische Differenzierung und die Zuordnung organisatorisch differenzierter Rollen zu Benutzern automatisiert.

Zunächst stellen wie in Abschnitt 9.1, »Herausforderungen und Lösungsansatz«, die Herausforderung dar, die zur Nutzung des Rollenmanagers führte, und erläutern, wie Sie ihr mit dem Rollenmanager in unterschiedlichen Szenarien begegnen können.

In Abschnitt 9.2, »Umsetzungsbeispiel für das Bereichsrollenkonzept«, stellen wir ein Konzept der Rollenmanager-Nutzung vor, das wir beim Kanton Zürich eingeführt haben. In Abschnitt 9.3, »Integration, Einschränkungen und Perspektiven«, zeigen wir die Integration

mit SAP BusinessObjects Access Control und gehen auf Einschränkungen und Perspektiven ein.

9.1 Herausforderung und Lösungsansatz

In einem System, in dem hochgradige organisatorische Differenzierung erforderlich ist, gelangen klassische Ableitungskonzepte an ihre wirtschaftliche Grenze: Rein rechnerisch wächst die Zahl möglicher Ableitungen mit der Zahl der zur Verfügung stehenden Ausprägungen der Organisationsebenen (z. B.: Anzahl Rollen * Buchungskreise * Kostenstellen * Werke * YYY) exponentiell. Aus diesem Grund sind viele Kunden zu mehr oder minder angemessen differenzierenden Wertrollenkonzepten übergegangen oder haben das Wertrollenkonzept mit dem Ableitungskonzept kombiniert.

Um die organisatorische Differenzierung effizient und standardisiert durchführen zu können, wurde für die Lösung *SAP for Defense Forces and Public Security* (DFPS) der Rollenmanager (*Role Generator*) entwickelt. Der Rollenmanager steht seit Release ECC 6.0 auch im Standard zur Verfügung.

Um eine Vorstellung davon zu bekommen, wie eine hochgradige organisatorische Differenzierung effizient bewerkstelligt werden kann, kann man die Besonderheiten der DFPS betrachten: Hier muss für zehntausende von Benutzern gewährleistet werden können, dass diese genau die Berechtigungen bekommen, die ihrer Einheit zugewiesen sind. Das gilt besonders für die Verwendung der Einheit im Frieden, im Übungsfall, im Einsatz oder im Verteidigungsfall. Es gilt aber ebenso für die Versorgung der Einheit während dieser Verwendung. Die notwendigen organisatorischen Differenzierungskriterien sind Werke, Buchungskreise, Finanzkreise, Kostenstellen, Einkäufergruppen, Lagerorte, Verantwortungsbereiche und viele weitere Merkmale der Logistik, der Produktionsplanung, des Rechnungswesens und der weiteren genutzten Applikationen.

Darüber hinaus muss ein Wechsel sämtlicher organisatorischen Berechtigungen effektiv von heute auf morgen möglich sein. Wenn eine Einheit in einen Einsatz oder eine Übung geschickt wird, ändern sich die Versorgungsbeziehungen der Einheit ebenso wie die administrativen Beziehungen. Das kann Auswirkungen auf alle Beziehungen der Organisationsebenen haben.

Genau das ermöglicht der Rollenmanager, der in der DFPS ausschließlich auf dem SAP ERP HCM-Organisationsmanagement beruht. Außerhalb der DFPS sind verschiedene weitere Lösungen auch ohne das Organisationsmanagement möglich. Der Fokus dieser Lösungen liegt ebenfalls auf der hochgradigen organisatorischen Differenzierung und der zügigen Umsetzung auch umfassender organisatorischer Änderungen.

Konkrete Herausforderung

Die Herausforderung besteht darin, dass für jeden Benutzer Berechtigungen bereitgestellt werden, die sowohl die funktionale Differenzierung als auch die organisatorische Differenzierung detailliert umsetzen. Tatsächlich ist dies nur der kleinere Teil der Anforderung, denn um diese Differenzierung effizient umzusetzen, müssen außerdem die folgenden drei Voraussetzungen erfüllt sein:

- Es sollen nur die erforderlichen Rollen angelegt werden.
- Sowohl funktionale als auch organisatorische Berechtigungen müssen gruppiert verwaltet werden können, d. h., nicht der einzelne Benutzer, sondern immer Gruppen von Funktionen und Organisationsmerkmalen sollen verwaltet werden (wie im Rollenkonzept üblich).
- Die richtigen Berechtigungen sollen automatisch dem Benutzer zugeordnet werden.

Lösungsansatz

Um der Herausforderung zu begegnen, benötigt der Rollenmanager also Informationen in drei Bereichen:

- funktionale Berechtigung
- organisatorische Berechtigung
- Benutzerzuordnungen

Diese drei Bereiche werden wir im Folgenden darstellen.

Funktionale Berechtigung

Dem Benutzer werden (indirekt oder direkt) weiterhin funktionale Rollen zugewiesen. Die Besonderheit dieser funktionalen Rolle besteht darin, dass alle Organisationsebenen, die für die organisatorische Differenzierung genutzt werden, ungepflegt bleiben. Dies ist der einzige Unterschied zu normalerweise zugeordneten Einzelrollen. Die so ausgeprägte Rolle enthält also ausnahmslos alle Berechtigungsobjekte, die die »normale« Einzelrolle auch enthalten würde. Ebenso sind alle Felder ausgeprägt, eben nur die relevanten Organisationsebenen nicht.

Organisatorische Berechtigung

Die zweite Information, die der Rollenmanager benötigt, ist die organisatorische Berechtigung. Um diese Information zu erhalten, stehen drei unterschiedliche Möglichkeiten bereit:

- **Rollenmanager OM**
  Unter Nutzung der indirekten Rollenzuweisung kann die Information aus den Objekten des Organisationsmanagements (OM) von SAP ERP HCM genutzt werden. Diese Möglichkeit wird im Folgenden als *Rollenmanager OM* bezeichnet.
- **Bereichsrollenkonzept**
  Unter Nutzung eines neuen Rollentyps, der Bereichsrolle, können die Informationen aus den Bereichsrollen verwendet werden. Diese Möglichkeit wird im Folgenden als *Bereichsrollenkonzept* bezeichnet.
- **Freie Rollenmanager-Adaption**
  Die dritte Möglichkeit ist die Nutzung kundeneigener Tabellen, diese Möglichkeit kann als *freie Rollenmanager-Adaption* bezeichnet werden und wird nicht weiter erläutert.

Benutzerzuordnung

Die dritte Information, die Benutzerzuordnung, ist konzeptabhängig. In beiden Konzepten müssen die funktionale Berechtigung und die organisatorische Berechtigung durch die Benutzerzuordnung ermittelt werden:

In der Rollenmanager-OM-Option wird die Zuordnung der funktionalen Rolle zum Benutzer über Auswertungswege ermittelt. Die Zuordnung der Organisationswerte wird ebenfalls über Auswertungswege ermittelt. Dabei werden aus den Objekten, zu denen der Benutzer in SAP ERP HCM-OM eine Verknüpfung hat, die dort gepflegten Organisationsebenen ausgewertet. Somit stehen die Werte für die Funktionen und die Organisation in Verbindung zu einem konkreten Benutzer zur Verfügung.

Im Bereichsrollenkonzept sind sowohl die Bereichsrollen als auch die funktionalen Rollen direkt dem Benutzer zugeordnet. Mit anderen Worten: Die Beziehungen müssen nicht ermittelt, sondern ausgewertet werden. Somit stehen die Werte für die Funktionen und die Organisation in Verbindung zu einem konkreten Benutzer unmittelbar zur Verfügung.

Aus der Kombination der funktionalen Rolle entweder mit den Werten von SAP ERP HCM-OM oder der Bereichsrolle legt der Rollenmanager eine neue, benutzerindividuelle Rolle an, die Zuständigkeitsrolle oder Rollenmanager-Rolle. Diese Rolle weist der Rollenmanager direkt dem Benutzer zu.

Zuständigkeitsrolle/Rollenmanager-Rolle

9.1.1 Rollenmanager OM

Dem Benutzer sind in diesem Konzept indirekt funktionale Rollen zugewiesen. Für die Systematik der indirekten Rollenzuordnung und der Auswertewege verweisen wir auf Kapitel 8, »Rollenzuordnung über das Organisationsmanagement«. Aus der Zuweisung der funktionalen Rollen wird ermittelt, welche organisatorischen Berechtigungen der Rollenmanager zuordnen muss. Wie das funktioniert, werden wir Ihnen im Folgenden erläutern.

Funktionale Rolle

Die funktionalen Rollen enthalten mit Ausnahme der relevanten Organisationsebenen voll ausgeprägte Berechtigungsobjekte. Dadurch, dass die Organisationsebenen nicht ausgeprägt sind, ist eine Reihe von Berechtigungsobjekten unvollständig in der funktionalen Rolle ausgeprägt.

In einer Rolle zur Pflege von FI-Belegen wäre zum Beispiel das Berechtigungsobjekt F_BKPF_BUK in der Ausprägung, die in Tabelle 9.1 gezeigt wird, enthalten.

Berechtigungsobjekt	Berechtigungsfeld	Berechtigungswert
F_BKPF_BUK	ACTVT	01, 02, 03
F_BKPF_BUK	BUKRS	$BUKRS

Tabelle 9.1 Exemplarische Ausprägung eines Berechtigungsobjekts in einer funktionalen Rolle

Der Rollenmanager liest diese Information und überträgt sie in die benutzerindividuelle Zuständigkeitsrolle.

Organisationsebenen aus den SAP ERP HCM-OM-Objekten und der Zuständigkeitsrolle

Aus den Organisationsmanagementobjekten ermittelt der Rollenmanager über Auswertepfade, welche Buchungskreise dem Benutzer indirekt zugeordnet sind. Im folgenden Beispiel ist das der Buchungskreis 1000. Mit diesem Buchungskreiswert prägt der Rollenmanager die Zuständigkeitsrolle aus, sodass sich das in Tabelle 9.2 dargestellte Bild ergibt.

Berechtigungsobjekt	Berechtigungsfeld	Berechtigungswert
F_BKPF_BUK	ACTVT	01, 02, 03
F_BKPF_BUK	BUKRS	1000

Tabelle 9.2 Ausprägung in der Zuständigkeitsrolle

Der Rollenmanager prägt das Berechtigungsfeld und nicht die Organisationsebene aus. Das ist notwendig, um etwaige Differenzierungen nach Tätigkeiten zu ermöglichen, z. B. wenn in einem Buchungskreis nur angezeigt, in einem anderen gebucht und im dritten freigegeben werden soll.

Diese Ausprägung nimmt der Rollenmanager für alle Berechtigungsobjekte mit offenen Organisationsebenen aus allen dem Benutzer zugeordneten Rollen vor. Die so erzeugte benutzerindividuelle Rolle (genau eine) wird dem Benutzer direkt zugewiesen.

Mehrere funktionale Rollen

In diesem Konzept können mehrere funktionale Rollen indirekt zugeordnet sein.

Ablauf im OM-Szenario

Wie dem oberen Teil der Abbildung 9.1 zu entnehmen ist, kombiniert der Rollenmanager Informationen aus der indirekten Zuordnung von funktionalen Rollen (in der Abbildung F_ROLLE) in SAP ERP HCM-OM mit den Informationen über die Organisationsebene aus SAP ERP HCM-OM in einer Zuständigkeitsrolle (in der Abbildung Z_ROLLE). Im zweiten Schritt (im unteren Teil der Abbildung 9.1) ordnet der Rollenmanager diese Rolle direkt dem Benutzer zu.

Restriktion des Rollenmanager-OM-Ansatzes

Im Standard von SAP ERP HCM-OM sind nur wenige Organisationsebenen mit den HCM-Objekten verknüpft. Bei diesen handelt es sich überwiegend um Organisationsebenen und Merkmale (insbesondere Kostenstellen) aus dem Rechnungswesen. Weitere Verknüpfungen müssten manuell angelegt werden, eine Automatisierung der Verknüpfung wäre mit erheblichem Aufwand verbunden. In der DFPS sind umfänglich weitere Organisationsebenen mit den Objekten verknüpft. Dies ist ein wesentliches Merkmal der dort verfügbaren Workbench-Organisation. Diese umfangreichen weiteren Verknüpfungen sind im Standard nicht enthalten.

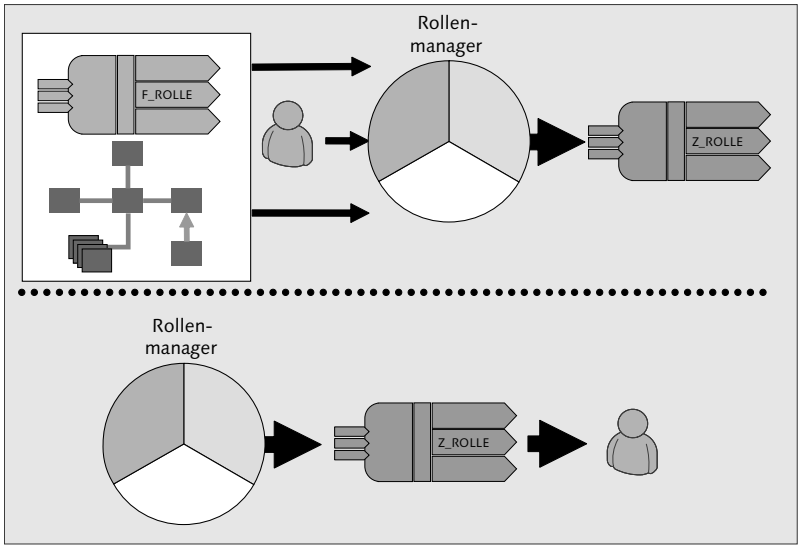


Abbildung 9.1 Funktionalität des Rollenmanagers OM

9.1.2 Bereichsrollenkonzept

Das in diesem Abschnitt vorgestellte Konzept wurde beim Kanton Zürich integriert mit SAP BusinessObjects Access Control eingeführt. Das Bereichsrollenkonzept basiert ebenfalls auf der Zuweisung von funktionalen Rollen. Die notwendigen organisatorischen Berechtigungen werden durch Bereichsrollen zugewiesen und durch den Rollenmanager in Zuständigkeitsrollen umgesetzt, wie wir nachfolgend darstellen werden.

Die funktionale Berechtigung muss auch hier, wie im Rollenmanager-OM-Ansatz, über eine funktionale Rolle vergeben werden. Das Bereichsrollenkonzept setzt für die organisatorische Differenzierung auf dem neuen Konstrukt der Bereichsrolle auf. Diese setzt wiederum auf zwei neuen Berechtigungsobjekttypen auf:

- dem Organisationsebenenobjekt
- dem Kategorisierungsobjekt
- Im Folgenden werden die Rollentypen und die Berechtigungsobjekttypen dargestellt.

Funktionale Rolle

Die funktionale Rolle wird in diesem Fall dem Benutzer direkt zugeordnet. Inhaltlich unterscheidet sich die funktionale Rolle dieses Konzepts nur in einem Punkt von der Darstellung im Rollenmanager-OM-Konzept. Jeder funktionalen Rolle muss das Kategorisierungsobjektzugeordnet und für die gewünschte Verwendung (Lesen, Schreiben oder Buchen) ausgeprägt werden.

Organisationsebenenobjekt

Das Organisationsebenenobjekt enthält jeweils genau eine Organisationsebene. Zurzeit wird es als kundeneigenes Objekt angelegt. Es sind also nur so viele Objekte anzulegen, wie Organisationsebenen im System zur organisatorischen Differenzierung genutzt werden sollen. Ein Beispiel für ein Organisationsebenenobjekt finden Sie in Tabelle 9.3.

Berechtigungsobjekt	Berechtigungsfeld	Berechtigungswert
Z_ BUKRS	BUKRS	$BUKRS

Tabelle 9.3 Beispiel: Organisationsebenenobjekt »Buchungskreis«

Kategorisierungsobjekt

In vielen Fällen möchte man bestimmte funktionale und organisatorische Zuständigkeiten auf Anzeige-, Pflege- oder Buchungsberechtigungen beschränken. Dies macht die Unterteilung der Rollen in drei Kategorien notwendig: Rollen mit reinen Anzeigeberechtigungen, Rollen mit Pflegeberechtigungen und Rollen mit Buchungsberechtigungen.

Zur technischen Kennzeichnung der Rollen wird das sogenannte *Kategorisierungsobjekt* eingeführt. Dieses Objekt muss als kundeneigenes Objekt (siehe Abschnitt 7.9.2, »Berechtigungsobjekte anlegen«) angelegt werden. Es enthält ebenfalls nur ein einziges Feld, das Feld ACTVT (Aktivität).

Bereichsrolle

Die Bereichsrolle enthält ausschließlich Organisationsebenenobjekte sowie das Kategorisierungsobjekt (siehe Tabelle 9.4). In den Organisationsebenenobjekten werden alle Organisationsebenenwerte gepflegt, die für die in einem bestimmten Organisationsbereich tätigen Benutzer erforderlich sind. Die Definition eines Bereichs und damit die Zusammenstellung der erforderlichen Organisationsebenen ist immer kundenspezifisch. Die Bereichsrolle wird direkt dem Benutzer zugeordnet.

Berechtigungsobjekt	Berechtigungsfeld	Berechtigungswert
Z_ BUKRS	BUKRS	1000
Z_ KOKRS	KOKRS	1000
Z_ ACTVT	ACTVT	01

Tabelle 9.4 Ausprägung der Bereichsrolle

Die in Tabelle 9.4 dargestellte Ausprägung ist vereinfacht, tatsächlich wird in der Bereichsrolle die Organisationsebene in den Organisationsebenen und nicht im Feld ausgeprägt.

Organisationsebene im Berechtigungsobjekt der Zuständigkeitsrolle

Mit den Werten der Bereichsrolle und der funktionalen Rolle prägt der Rollenmanager die Zuständigkeitsrolle aus. Zu diesem Zweck muss er die Ausprägung des Kategorisierungsobjekts in der Bereichsrolle und in der funktionalen Rolle jeweils für die gleiche Aktivität nutzen, sodass sich das in Tabelle 9.5 dargestellte Bild ergibt.

Berechtigungsobjekt	Berechtigungsfeld	Berechtigungswert
F_BKPF_BUK	ACTVT	01
F_BKPF_BUK	BUKRS	1000

Tabelle 9.5 Ausprägung in der Zuständigkeitsrolle

Der Rollenmanager prägt auch in diesem Konzept tatsächlich das Berechtigungsfeld und nicht die Organisationsebene aus. Auch in diesem Konzept wird die Zuständigkeitsrolle (genau eine) durch den Rollenmanager direkt dem Benutzer zugewiesen.

Mehrere funktionale Rollen und Bereichsrollen

Im Bereichsrollenkonzept können mehrere funktionale Rollen und Bereichsrollen direkt zugeordnet sein. Mehrere Bereichsrollen sind sinnvoll, um für verschiedene Bereiche der Organisation zwischen lesenden und anderen Berechtigungen unterscheiden zu können.

Ablauf im Bereichsrollenkonzept

Wie dem oberen Teil der Abbildung 9.2 zu entnehmen ist, kombiniert der Rollenmanager Informationen aus der funktionalen Rolle (in der Abbildung F_ROLLE) mit den Informationen der Bereichsrolle (in der Abbildung B_ROLLE) in einer Zuständigkeitsrolle (in der Abbildung Z_ROLLE). Im zweiten Schritt ordnet der Rollenmanager diese Rolle direkt dem Benutzer zu.

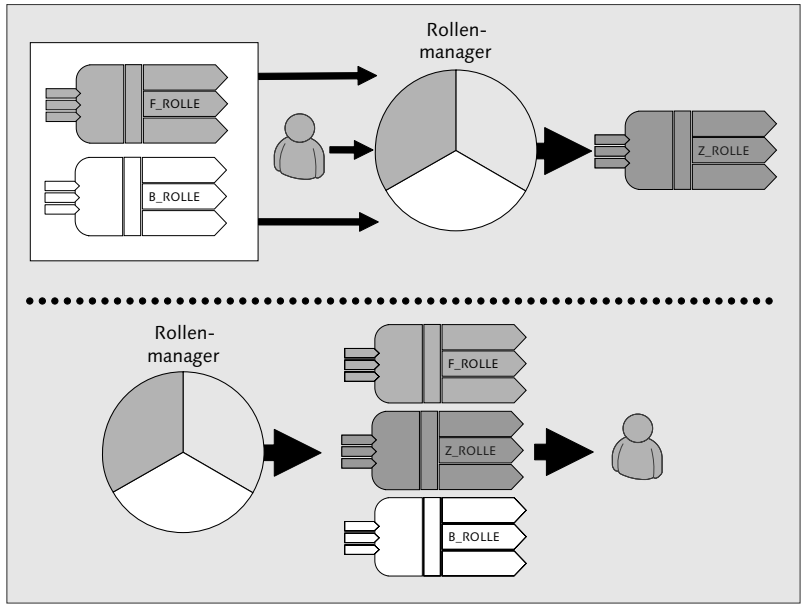


Abbildung 9.2 Bereichsrollenkonzept – Rollenmanager

9.1.3 Kombination von Bereichsrollen und OM

Die beiden Grundkonzepte Rollenmanager OM und Bereichsrollenkonzept lassen sich kombinieren. Die Zuordnung einer Bereichsrolle kann also auch an ein Objekt des Organisationsmanagements ungleich dem Benutzer (der im Organisationsmanagement auch ein Objekt ist, siehe Kapitel 8, »Rollenzuordnung über das Organisationsmanagement«) erfolgen.

In diesem kombinierten Konzept sollte die Zuordnung der funktionalen Rollen weitaus überwiegend über die indirekte Rollenzuordnung erfolgen. Dies ist in Abbildung 9.3 dargestellt. Die Zuordnung der Bereichsrollen zu Objekten von SAP ERP HCM-OM ist sinnvoll, um z. B. lesende Zugriffe ❶ für einen größeren Bereich der Organisation »hoch« in der Hierarchie zu vergeben, schreibende oder buchende Berechtigungen »tief« ❷, also nah an der Position, und spezielle organisatorische Berechtigungen an der Stelle oder der Planstelle ❸.

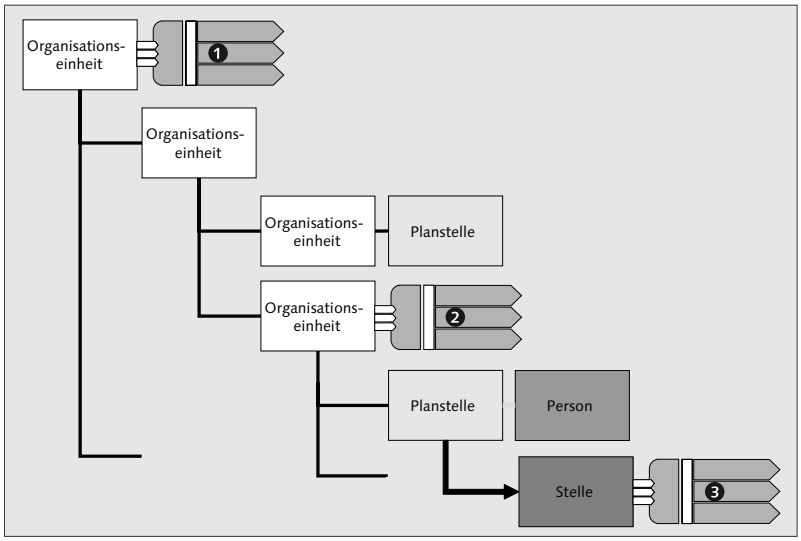


Abbildung 9.3 Bereichsrollen in der Organisationshierarchie

9.2 Umsetzungsbeispiel für das Bereichsrollenkonzept

Das Bereichsrollenkonzept kann kundenindividuell umgesetzt werden. Als Beispiel beschreiben wir die Implementierung des Bereichsrollenkonzepts im Kanton Zürich. Das Beispiel gibt die konkrete Umsetzung technisch detailliert wieder, um Sie in die Lage zu versetzen, das vorher beschriebene Konzept in Bezug auf notwendige Berechtigungsobjekte, Rollen und Einstellungen detaillierter nachzuvollziehen.

Notwendige Berechtigungsobjekte

Für das Bereichsrollenkonzept werden das Organisationsebenenobjekt und das Kategorisierungsobjekt benötigt. Diese sind in einer kundeneigenen Objektklasse als kundeneigene Berechtigungsobjekte angelegt worden (siehe Abbildung 9.4).

Für die in der Beispielimplementierung eingesetzte Methode war es erforderlich, dass das Kategorisierungsobjekt Z_ACTVT heißt und lediglich das Feld ACTVT enthält. Es war sinnvoll, die erlaubten Aktivitäten auf die gewünschte Differenzierung/Kategorisierung zu begrenzen (siehe Abbildung 9.5). In diesem Beispiel wird funktional zwischen STAMMDATENPFLEGE (gekennzeichnet durch Aktivität 01), ANZEIGEN (gekennzeichnet durch Aktivität 03) und BUCHEN (gekenn-

zeichnet durch Aktivität 10) unterschieden. Die Aktivitäten in diesem Objekt stellen lediglich das Attribut *Kategorie*. Dieses wird in funktionalen Rollen und Bereichsrollen gepflegt. Das spätere Mapping erfolgt über die Attributierung mithilfe dieses Objekts und nicht über etwaige andere Aktivitätsausprägungen in der funktionalen Rolle.

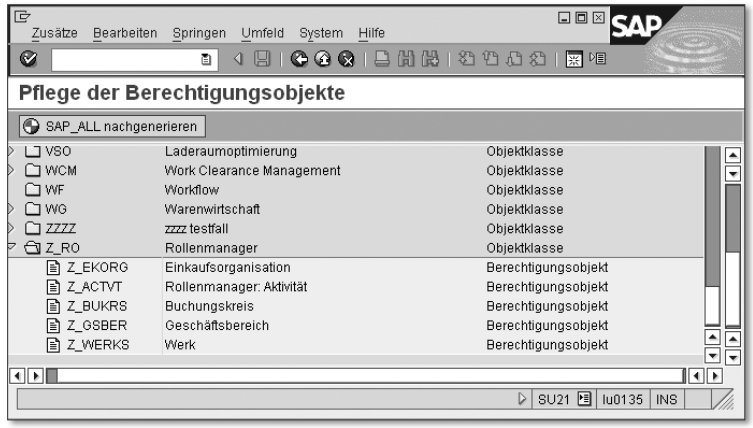


Abbildung 9.4 Objekte für den Rollenmanager

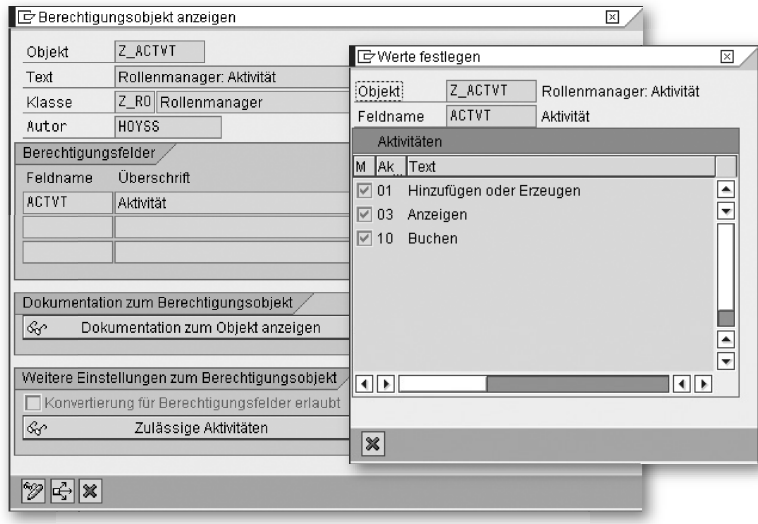


Abbildung 9.5 Einschränkung der zulässigen Aktivitäten

Die Organisationsebenenobjekte enthalten ausschließlich Organisationsebenen. In der Umsetzung haben wir es als sinnvoll erachtet, für

jedes Objekt genau eine Organisationsebene vorzusehen (siehe Abbildung 9.6).

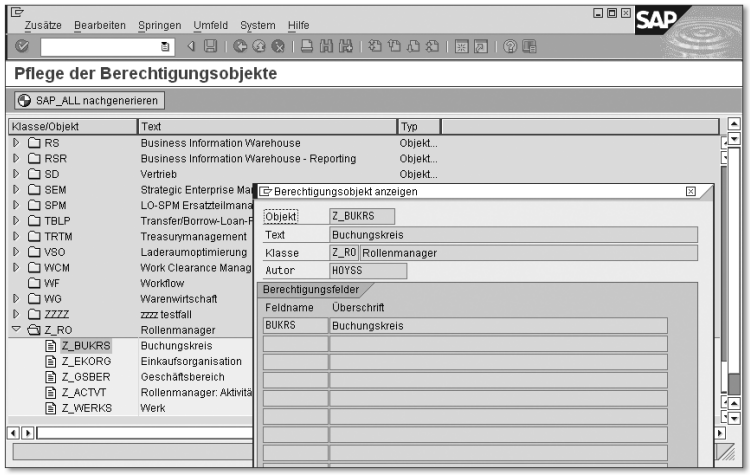


Abbildung 9.6 Organisationsebenenobjekt

Funktionale Rolle

Die funktionale Rolle enthält alle Transaktionen und funktional notwendigen Berechtigungsobjekte. Zusätzlich enthält die Rolle das Berechtigungsobjekt Z_ACTVT. Die für die Differenzierung genutzten Organisationsebenen werden nicht ausgeprägt. Eine einfache Rolle zur logistischen Pflege von Kreditoren ist in Abbildung 9.7 dargestellt.

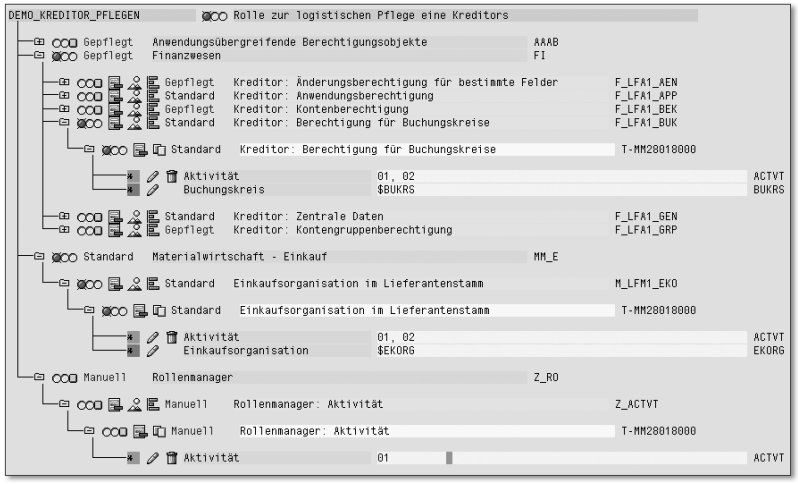


Abbildung 9.7 Beispiel eines Profils einer funktionalen Rolle

Vergeben sind die Transaktionen Kreditor anlegen (logistische Sicht) und Kreditor ändern (logistische Sicht). Die Organisationsebenen enthalten den automatischen Platzhalter. Das Objekt Z_ACTVT ist ausgeprägt mit 01, da die 01 für Anlegen/Ändern steht.

Für das Beispiel (die folgende Kombination in unserem Beispiel-Benutzerstammsatz) wird eine weitere sinngemäße Rolle für die Anzeige von Kreditoren benötigt. Diese Rolle ist auf dem Objekt Z_ACTVT mit 03 für Anzeigen ausgeprägt (aber hier nicht im Einzelnen dargestellt).

Bereichsrolle

Im Beispiel aus Abbildung 9.7 werden zwei Organisationsebenen benutzt, Einkaufsorganisation und Buchungskreis. Im Regelfall kommen weitere hinzu, jedoch soll hier aus Gründen der Übersichtlichkeit nur von diesen beiden ausgegangen werden.

Möglich sind für die organisatorische Differenzierung folgende Fälle:

- **Einfache Kombination – starre Zuordnung**
  Die Einkaufsorganisation entspricht dem Buchungskreis. In diesem Fall muss nur eine Bereichsrolle pro Aktivitätskategorie und Kombination Buchungskreis – Einkaufsorganisation angelegt werden.
- **Unterschiedliche eindeutige Kombination – starre Zuordnung**
  Es gibt immer eine logische Verbindung von Einkaufsorganisation und Buchungskreis. In diesem Fall muss nur eine Bereichsrolle pro Aktivitätskategorie und Kombination Buchungskreis – Einkaufsorganisation angelegt werden. Es werden aber mehr Rollen als im ersten Fall erzeugt.
- **Fallweise Kombination – freie Zuordnung**
  Buchungskreis und Einkaufsorganisation müssen fallweise (pro Benutzer und Funktion) verbunden werden. Sie müssen für die Buchungskreise und die Einkaufsorganisationen jeweils je Aktivitätskategorie eigene Bereichsrollen anlegen.

In unserem Beispiel soll die volle Flexibilität, also der dritte Fall, verfolgt werden. Es werden somit pro Buchungskreis und pro Einkaufsorganisation folgenden Rollen benötigt:

- Bereichsrolle Anzeigen
- Bereichsrolle Pflegen
- Bereichsrolle Buchen

Die Rollen für das Buchen sind im konkreten Beispiel nicht relevant, da es um die funktionalen Rollen *Kreditor pflegen* und *Kreditor anzeigen* geht.

Die Rolle *Buchungskreis pflegen* enthält das Berechtigungsobjekt Z_BUKRS (Buchungskreis) und das Objekt Z_ACTVT. In Abbildung 9.8 ist die Bereichsrolle für den Buchungskreis DEMO und die Aktivität 01 (Anlegen/Ändern) ausgeprägt. Der Buchungskreis wird über die Standardorganisationsebenenpflege ausgeprägt.

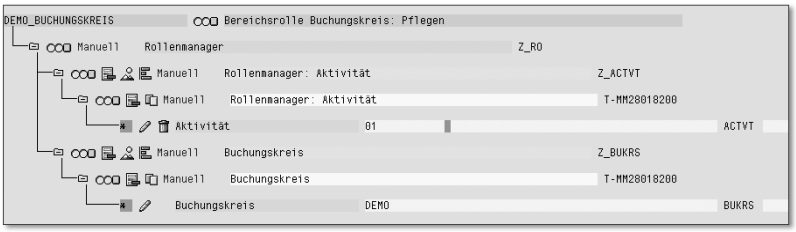


Abbildung 9.8 Bereichsrolle »Buchungskreis pflegen«

Kombination der Rollen im Benutzerstammsatz

Im Benutzerstammsatz werden für das Beispiel die funktionalen Rollen *Kreditor pflegen* und *Kreditor anzeigen* sowie die entsprechenden Bereichsrollen zusammengeführt (siehe Abbildung 9.9).

Abbildung 9.9 Kombination im Benutzerstammsatz

Aus der Kombination im Benutzerstammsatz ergibt sich das in Tabelle 9.6 dargestellte Bild. Die funktionalen Rollen sind auf den Gegenstand des Beispiels reduziert, andere Objekte werden nicht aufgeführt.

Rolle	Objekt	Feld	Wert	Org.Ebene
BUCH.KREIS_ANZEIGEN	Z_ACTVT	ACTVT	03	
BUCH.KREIS_ANZEIGEN	Z_BUKRS	BUKRS	$BUKRS	DEMO
BUCH.KREIS_PFLEGEN	Z_ACTVT	ACTVT	01	
BUCH.KREIS_PFLEGEN	Z_BUKRS	BUKRS	$BUKRS	SARA
EINK.ORG_ANZEIGEN	Z_ACTVT	ACTVT	03	
EINK.ORG_ANZEIGEN	Z_EKORG	EKORG	$EKORG	COOP
EINK.ORG_PFLEGEN	Z_ACTVT	ACTVT	01	
EINK.ORG_PFLEGEN	Z_EKORG	EKORG	$EKORG	REWE
(…)				
KREDITOR_ANZEIGEN	F_LFA1_BUK	BUKRS	$BUKRS	
KREDITOR_ANZEIGEN	F_LFA1_GEN	ACTVT	03	
KREDITOR_ANZEIGEN	F_LFA1_GRP	ACTVT	03	
KREDITOR_ANZEIGEN	F_LFA1_GRP	KTOKK	*	
KREDITOR_ANZEIGEN	M_LFM1_EKO	ACTVT	03	
KREDITOR_ANZEIGEN	M_LFM1_EKO	EKORG	$EKORG	
KREDITOR_ANZEIGEN	Z_ACTVT	ACTVT	03	
(…)				
KREDITOR_PFLEGEN	F_LFA1_BUK	ACTVT	01, 02	
KREDITOR_PFLEGEN	F_LFA1_BUK	BUKRS	$BUKRS	
KREDITOR_PFLEGEN	M_LFM1_EKO	ACTVT	01, 02	
KREDITOR_PFLEGEN	M_LFM1_EKO	EKORG	$EKORG	
KREDITOR_PFLEGEN	Z_ACTVT	ACTVT	01	

Tabelle 9.6 Bereichsrollen und funktionale Rollen im Beispiel

Aus diesen Werten kombiniert der Rollenmanager nun die Zuständigkeitsrolle. Dazu muss das – zurzeit noch – kundeneigene Programm ausgeführt werden. In Abbildung 9.10 sehen Sie, dass dieses Programm entweder über eine Namenskonvention oder über das vergebene Objekt Z_ACTVT die Rollen kombiniert.

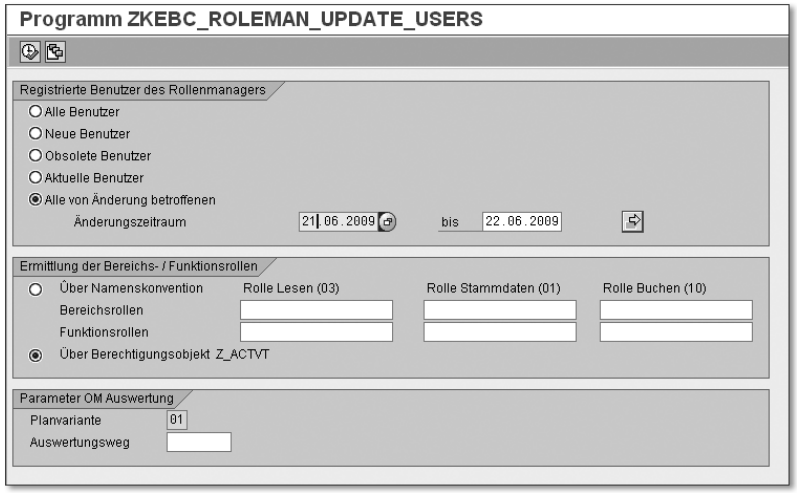


Abbildung 9.10 Einstiegsbildschirm des Rollenmanagers

Beachten Sie bei der Umsetzung über Namenskonventionen, dass die Rollen einer Kategorie gleich beginnen müssen, um die generische Ausprägung möglich zu machen (siehe Tabelle 9.7).

Rolle	Präfix
Bereichsrolle Lesen	Z_BL
Bereichsrolle Buchen	Z_BB
Bereichsrolle Anlegen/Ändern	Z_BA
funktionale Rolle Lesen	Z_FL
funktionale Rolle Buchen	Z_FB
funktionale Rolle Anlegen/Ändern	Z_FA

Tabelle 9.7 Mögliche Präfixe im Rollennamen

Der Rollenmanager generiert automatisch genau eine Zuständigkeitsrolle im SAP-Namensraum. Diese ist ausgeprägt, wie in Tabelle 9.8 dargestellt. Beachten Sie, dass die früheren Organisationsebenenwerte in dieser Rolle im Feld eingetragen werden.

Rollenname	Objekt	Feld	Wert
SAP_RM_EXAMPLE	F_LFA1_BUK	ACTVT	3
SAP_RM_EXAMPLE	F_LFA1_BUK	BUKRS	DEMO

Tabelle 9.8 Role-Manager-Rolle

Rollenname	Objekt	Feld	Wert
SAP_RM_EXAMPLE	F_LFA1_BUK	ACTVT	3
SAP_RM_EXAMPLE	F_LFA1_BUK	BUKRS	$BUKRS
SAP_RM_EXAMPLE	F_LFA1_BUK	ACTVT	1
SAP_RM_EXAMPLE	F_LFA1_BUK	ACTVT	2
SAP_RM_EXAMPLE	F_LFA1_BUK	BUKRS	SARA
SAP_RM_EXAMPLE	F_LFA1_BUK	ACTVT	1
SAP_RM_EXAMPLE	F_LFA1_BUK	ACTVT	2
SAP_RM_EXAMPLE	F_LFA1_BUK	BUKRS	$BUKRS
SAP_RM_EXAMPLE	M_LFM1_EKO	ACTVT	3
SAP_RM_EXAMPLE	M_LFM1_EKO	EKORG	$EKORG
SAP_RM_EXAMPLE	M_LFM1_EKO	ACTVT	3
SAP_RM_EXAMPLE	M_LFM1_EKO	EKORG	COOP
SAP_RM_EXAMPLE	M_LFM1_EKO	ACTVT	1
SAP_RM_EXAMPLE	M_LFM1_EKO	ACTVT	2
SAP_RM_EXAMPLE	M_LFM1_EKO	EKORG	$EKORG
SAP_RM_EXAMPLE	M_LFM1_EKO	ACTVT	1
SAP_RM_EXAMPLE	M_LFM1_EKO	ACTVT	2
SAP_RM_EXAMPLE	M_LFM1_EKO	EKORG	REWE

Tabelle 9.8 Role-Manager-Rolle (Forts.)

Die Feldwertausprägung in der Vervielfachung der Objekte zur funktionsbezogenen Ausprägung sehen Sie in Abbildung 9.11.

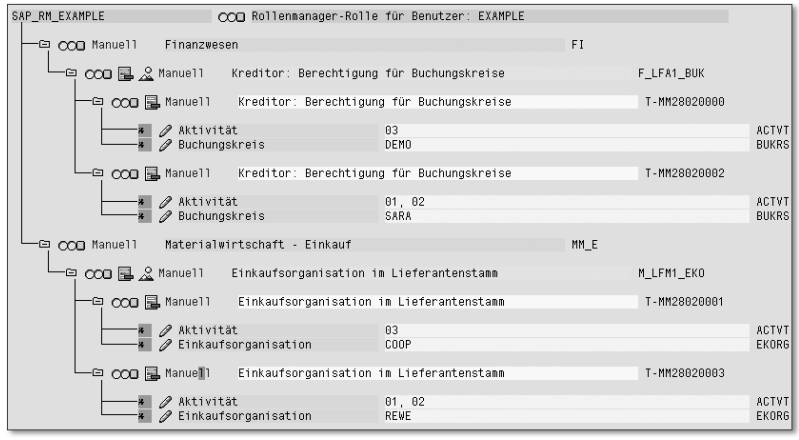


Abbildung 9.11 Rollenmanager-Rolle

9.3 Integration, Einschränkungen und Perspektiven

Integration mit SAP BusinessObjects Access Control

Im Kanton Zürich war es eine zusätzliche Herausforderung, den Rollenmanager mit SAP BusinessObjects Access Control zu verbinden. Damit wird sichergestellt, dass die organisatorischen Berechtigungen automatisiert generiert, die funktionalen Berechtigungen aber immer auch einer Risikoanalyse unterzogen werden.

Die Integration ist simpel: Sowohl die funktionale Rolle als auch die Bereichsrolle werden über das *Compliant User Provisioning* (CUP) beantragt. Der Rollenmanager nimmt die Generierung der Zuständigkeitsrolle nach der Zuweisung vor.

Einschränkungen

Der Rollenmanager ist ein reines ABAP-Werkzeug, das auf den Elementen der ABAP-Rollenpflege beruht. Deshalb können Sie ihn in keiner Non-ABAP-Lösung einsetzen. Darüber hinaus kann er auch nicht in ABAP-Lösungen, die nicht auf dem ABAP-Rollenkonzept beruhen, genutzt werden.

Perspektiven

Derzeit prüfen wir die Option, den Rollenmanager auch in SAP NetWeaver BW einzusetzen. Eine zwingende Bedingung dafür ist die Nutzung von Rollen für Analyseberechtigungen. Nur dann kann diese Funktionalität genutzt werden. Entsprechende Ansätze werden fallweise auch in weiteren Kontexten wie SAP CRM zu prüfen sein.

9.4 Fazit

Der Rollenmanager bewirkt eine signifikante Vereinfachung von Pflege und Administration in den Fällen, in denen eine hochgradige organisatorische Differenzierung erforderlich ist, die in der klassischen Ableitung zu einem exponentiellen Wachstum der Rollenanzahl führt.

Unter hochgradiger organisatorischer Differenzierung ist bei der Bewertung Folgendes zu verstehen: Es werden minimal drei Organisationsebenen (gegebenenfalls auch kundenspezifische wie die Kostenstelle) zur Differenzierung herangezogen.

Tabelle 9.9 verdeutlicht den exponentiell steigenden Nutzen des Bereichsrollenkonzepts im Vergleich zur klassischen Ableitung. Bei

der klassischen Ableitung sind im angegeben Mengengerüst 4.000.000 Rollen möglich, im Bereichsrollenkonzept hingegen nur 790.

Laufende Nummer	Merkmal/Objekt	Anzahl
1	funktionale Rollen	100
2	Buchungskreise	10
3	Werke	20
4	Kostenstellen	200
5	Summe: Kombinationsmöglichkeiten Organisationsebenen Nr. 2 * Nr. 3 * Nr. 4	40.000
6	funktionales Unterscheidungsmerkmal	3
7	Rollenmanager-Rollen (Nr. 2 + Nr. 3 + Nr. 4) * Nr. 6	690
8	Summe: max. Rollen Bereichsrollenkonzept Nr. 1 + Nr. 7	790
9	Summe: max. abgeleitete Rollen (Summe klassische Ableitung) Nr. 1 * Nr. 5	4.000.000

Tabelle 9.9 Ableitung versus Bereichsrollenkonzept

Neben der rein rechnerischen Argumentation hat das Bereichsrollenkonzept einen weiteren prozessualen Nutzen. Die Entscheidung über den funktionalen Zugriff »Was darf ein Nutzer?« kann losgelöst von der Entscheidung des organisatorischen Zugriffs »Wo darf ein Nutzer etwas?« getroffen werden.

Sofern Sie den Bedarf nach einer hochgradigen organisatorischen Differenzierung in SAP ERP haben, gibt es zum Rollenmanager nach unserer Einschätzung keine Alternative.