

# **Ausgesuchte Berechtigungsobjekte des SAP R/3 - Systems als Prüfungsansatz für die IV-Revision - Eine Übersicht -**

*Von Dipl.-Betriebswirt Christoph Wildensee, Hannover<sup>1</sup>*

## **1. Einführung**

Das SAP R/3 - System ist so umfangreich und vielschichtig wie kaum ein anderes DV-System mit dem Anspruch eines ganzheitlichen Charakters. Prüfungen in diesem Umfeld durchzuführen, ist nicht ganz unproblematisch. Erschwerend wirkt sich zum einen die große Anzahl von Verwaltungsobjekten wie Transaktionen, Profilen/Sammelprofilen, Rollen/Aktivitätsgruppen und Berechtigungsobjekten aus, zum anderen aber besonders auch die Semantik dieser Objekte, die sich in den Einzelausprägungen der einzustellenden Objektkriterien widerspiegeln. Weiterhin bedeutsam ist die Möglichkeit der Mehrfachverschachtelung von Profilen/Sammelprofilen über mehrere Iterationsstufen, die Berechtigungszuweisungen verschleiern kann.

Bisher ist es für den Revisor nicht immer eindeutig, welche Systemumgebungsparameter und Berechtigungsobjekte für ihn relevant sind. Die Betrachtung unterscheidet sich natürlich durch den Prüfungsansatz, d.h. prüft er als IV-Revisor im überwiegenden Bereich der Basis oder z.B. als kaufmännischer Revisor im Bereich Finanzwesen/Controlling/Kostenrechnung. Eine umfassende Übersicht über vorhandene relevante Berechtigungsobjekte und deren Ausprägungen ist bisher nicht vorhanden, so dass jeder Prüfer doch eher auf sich gestellt ist.

Dieser Artikel soll eine Übersicht über einige der wichtigsten Berechtigungsobjekte geben, die für die Prüfung der SAP-Basis und in einem späteren Schritt des Bereiches FI/CO relevant sind. Weiterhin sollen auch kurz die Problemstellungen dargelegt werden, die mit der Prüfung dieser Objekte verbunden sind. Umfassend ist natürlich auch diese Übersicht nicht, sie kann aber Hinweise für zukünftige Prüfungen geben.

## **2. SAP R/3 - Betrachtungsebene**

Bevor das Berechtigungsumfeld von SAP R/3 geprüft wird, sollte dem Revisor bewusst sein, was eine Prüfung in diesem Umfeld bedeutet. Die SAP R/3-Berechtigungsvergabe ist das Zusammenspiel von Transaktionen (Berechtigungsobjekt S\_TCODE [Feld TCD]) und Berechtigungsobjekten, zusammengefasst in Profilen/Sammelprofilen und diese wiederum in aufgabenorientierten Rollen/Aktivitätsgruppen.

Basis einer sinnvollen Berechtigungskonzeption ist somit in erster Linie das Berechtigungsobjekt, welches Profilen/Sammelprofilen zugewiesen wird. Ausschlaggebend ist die jeweilige Einzelausprägung der Kriteriensteuerung des Berechtigungsobjektes, welches somit über den Zugriff zu SAP-Ressourcen entscheidet.

Über die zielführende Definition von Aktivitätsgruppen/Rollen und Profilen/Sammelprofilen lässt sich streiten, so dass dies unternehmensspezifisch zu klären und nicht Thema dieses Artikels ist. Streiten kann man sich jedoch nicht über die Wirkung und notwendige restriktive Vergabe von Rechten auf einzelne kritische Berechtigungsobjekte der SAP-Module, so dass hier eine Auswahl kritischer Berechtigungsobjekte dargestellt werden soll, die für Revisoren von besonderer Bedeutung sind.

## **3. Besonderheiten beim Prüfungsvorgehen**

Zur Prüfung des SAP R/3-Umfeldes stehen mehrere Instrumentarien zur Verfügung. Zum einen die SAP-eigenen Mittel wie z.B. das Audit Information System (AIS; Transaktion SECR; releaseabhängig), welches in strukturierter Form die vorhandenen Auswertungsreports zur Verfügung stellt, natürlich das Reporting selbst, um notwendige ABAP's direkt aufzurufen (z.B. RSUSR002 o.ä.)

---

<sup>1</sup> C. Wildensee ist bei der Stadtwerke Hannover AG als IV-Revisor und stellvertr. Datenschutzbeauftragter tätig.

und die Systemverwalterfunktionen (z.B. Werkzeuge - Administration - Benutzerpflege - Berechtigung / Profile / Benutzer [...]Transaktionen SU0x).  
 Zum anderen kann z.B. auch SAPaudit als externes Prüfungswerkzeug zum Einsatz kommen, das vielfältige Auswertungsmöglichkeiten zur Verfügung stellt, die SAP direkt nicht bietet.

Zu Beginn einer Prüfung sollte die Analyse und Dokumentation des zu untersuchenden Systems stehen. Dieses erfolgt u.a. mit dem Report RSPARAM, der insbesondere in den Parametern login/..., DIR\_....., rdisp/....., rec/client und auth/.... geprüft werden sollte.

Bei der weiteren Vorgehensweise und der Nutzung der Instrumentarien ist in jedem Fall der Grundsatz der restriktiven Vergabe von Rechten zu beachten. Auch wenn dem Benutzer in R/3 zur Nutzung einer Berechtigung nicht jede Ausprägung zugedacht wurde (Transaktion + Berechtigungsobjekt + Einzelausprägung), sollten die Zuweisungen der Berechtigungsobjekte und Einzelausprägungen nicht freigiebig erfolgen.

#### 4. Ausgesuchte Berechtigungsobjekte

Die nachfolgenden Berechtigungsobjekte stehen hier als Auszug kritischer Objekte. Die Darstellung ist so zu lesen, dass links das Berechtigungsobjekt mit Beschreibung steht, rechts daneben die Steuerungsobjekte (Felder) und z.T. die Referenztablette, die die Ausprägung des Steuerungsfeldes definiert (kursiv dargestellt; einsehbar mit der Transaktion SE16), daneben als kritisch zu untersuchende Ausprägungen mit kurzer Bemerkung.

Natürlich ist auch die Kombination von Berechtigungsobjekten mit entsprechenden Einzelausprägungen wichtig, wie dies in der Tabelle vereinzelt angedeutet ist.

Die Suche nach Berechtigungsobjekten kann über "Werkzeuge - Administration - Benutzerpflege - Berechtigung - Info - Objektliste m. Doku" erfolgen. Hier sind die Objekte ausführlich dokumentiert.

#### Basisberechtigungsobjekt

Berecht.obj.		Feld 1 <i>Prüftabelle</i>	Feld 2 <i>Prüftabelle</i>	Feld 3 <i>Prüftabelle</i>	Feld 4 <i>Prüftabelle</i>	Feld 5 <i>Prüftabelle</i>
	Kritische Berechtigung	Krit. Feldwert	Krit. Feldwert	Krit. Feldwert	Krit. Feldwert	Krit. Feldwert
<b>S_GUI</b>		<b>ACTVT</b>				
GUI-Aktivitäten		<i>TACT/TACTZ</i>				
	Download von Reports und Tabellen	61				
<b>S_DEVELOP</b>		<b>ACTVT</b>	<b>DEVCLASS</b>	<b>OBJNAME</b>	<b>OBJTYPE</b>	<b>P_GROUP</b>
Entwicklerberechtigungen		<i>TACT/TACTZ</i>	<i>TDEVC</i>		<i>EUOBJ</i>	<i>TPGP</i>
Zur Anwendungsentwicklung ist zusätzlich ein Entwickler-schlüssel (Tabelle DEVACCESS) notwendig	Anlegen	01	Z*	Z* oder Y*	DYNP, FUGR, PROG, LDBA, TRAN, DEVC, DOMA, STRU, TAB*, VIEW, SQLT, SUSO, *	
	Ändern	02				
	Aktivieren/Generieren	07				
	Ausführen	16				
	Generalberecht.	*	*	*		*
Die hier zugrundeliegenden Objekte sind sehr vielfältig, so z.B. Dynpros, Funktionsbausteingruppen, Programme, Entwicklungsklassen, logische Datenbanken, Menüs, Transaktionen, Domänen/Strukturen/Tabellen, Views, Clustertabellen, Sperrobjekte usw.						

<b>S_RFC</b>		<b>ACTVT</b> <i>TACT/TACTZ</i>	<b>RFC_NAME</b>	<b>RFC_TYPE</b>		
RFC-Zugriffs- berechtigung	Ausführen eines Zugriffs	16	*	FUGR		
<b>S_TABU_CLI</b> Änderung mandanten- unabhängiger Tabellen  in Kombination	Zugriff auf mandatenunab- hängige Tab.	'X'				'X' sollte nur bei wenigen Usern vorkommen wie Admin
<b>S_TABU_DIS</b> Tabellenpflege		<b>ACTVT</b> <i>TACT/TACTZ</i>	<b>DICBERCLS</b> <i>s. TDDAT</i>			
S_TABU_CLI -> 'X' sollte mit S_TABU_DIS -> 02 nur bei Basis-Admin liegen, mit 03 bei Show-Usern (Revi, bDSB, ggf. BR)	Ändern von Tabellen der Basis	02	S*			
	Ändern von Tabellen Personal	02	P*, T5*			
	Generalberecht.	*	*			
<b>S_PATH</b> Filezugriff aus ABAP		<b>ACTVT</b> <i>TACT/TACTZ</i>	<b>FS_BRGRU</b> <i>s. SPTH / SPTHB</i>			Sollte bei keinem üblichen Nutzer zu finden sein.
Pflegeberecht.		02				
	Generalberecht.	*	*			
<b>S_BDC_MONI</b> Batch-Input- Berechtigung	Mappe einer best. Gruppe (u. Protokoll) ...		<b>BDCAKTI</b>	<b>BDCGROUPID</b> z.B. Gruppe RF* = Finanzbereich		
...für Hinter- grundverarbei- tung übergeben	ABTC					
...analysieren	ANAL					
...im Dialog abspielen	AONL					
...löschen	DELE					
...freigeben	FREE					
...sperrern/ entsperren	LOCK					
...reorganisieren	REOG					
Generalberecht.	*					

<b>S_BTCH_JOB</b>		<b>JOBACTION</b>	<b>JOBGROUP</b>			
Batch-Job-Steuerung	autom. Freigabe eigener Jobs	RELE				
Die Job-Steuerung ist als kritisch anzusehen, Beschränkung auf den aktuellen Mandanten.	Anz. alle Spoolaufträge	SP01				
	Anz. aller Verarbeitungsprotokolle	PROT				
	Anz. fremde Job-Def. und Details	SHOW				
	Löschen von Jobs (auch fremde)	DELE				
	Anz. fremder Spool-Aufträge	LIST				
in Kombination	Generalberecht.	*	*			
<b>S_BTCH_NAM</b>		<b>BTCUNAME</b>	Stellt die Berechtigung zur Verfügung, unter der ein Job abläuft.			
Angabe des Batch-Benutzernamens für Berechtigungsprüfung	Generalberecht.	*	Diese Kombination kommt insb. in Fachbereichen mit umfangreichen Batch-Input-Aktivitäten vor wie Finanz- und Pers.bereich.			
<b>S_BTCH_ADM</b>		<b>BTCADMIN</b>	Ausführen aller Operationen auf alle Jobs mandantenübergreifend, auch externe Programme in Job-Steps ausführen			
Batch-Administrator/ Job-Super-User	Generalberecht.	*	Nur für besondere Funktionsträger innerhalb der Fachbereiche sinnvoll -> Batch-Admin, Modul-Admin, System-Admin			
	Admin-Berecht.	Y (= Yes)				
<b>S_CTS_ADMI</b>		<b>CTS_ADM FCT</b>	Diese Berechtigung sollte ausschließlich in der Hand der Basis-Admin. liegen.			
Administration des Change & Transport Systems	Änderung der Systemänderbarkeit	SYSC				
	Pflege der Steuertabellen (auch TCODE SE03 Work BenchOrgan.)	TABL				
	Auslösen von Importen (Transp.Mngm System)	IMPT, IMPA, IMPS				
	Initialisierung des WBO nach Systemkopie (TCODE SE06)	INIT				
	Generalberecht.	*				
<b>S_C_FUNCT</b>		<b>ACTVT</b>	<b>CFUNCNAME</b>	<b>PROGRAM</b>		restriktive Vergabe; nur für Basis-Admin
direkter Aufruf von C-Kernel-Funktionen aus ABAP	Ausführen	16				
	Audit Konf.			RSAUCONF		
	Generalberecht.	*	*	*		

<b>S_CLNT_IMP</b> Dateiimport bei Mandantenkopie		<b>ACTVT</b> <i>TACT/TACTZ</i>				
	Generalberecht. Importieren	* 60				
<b>S_DATASET</b> Berechtigung zum Dateizugriff auf Betriebssystemebene; auch Berechtigung zur Benutzung von BS-Kommandos als Dateifilter		<b>ACTVT</b> <i>TACT/TACTZ</i>	<b>FILENAME</b>	<b>PROGRAM</b>	sollte auf einige wenige bekannte Programme beschränkt werden. -> z.B. RSWATCH0	
	Schreibender Zugriff	34	auf alle Dateien auf BS-Ebene = *	z.B. Finanzber. RF* und ZF*		
	Schreibender Zugriff mit Filter	A7				
<b>S_ENQUE</b> Anzeigen und Löschen von Sperreinträgen BObjekt für Administration.		<b>S_ENQ_ACT</b>				
	Anz. fremder Sperrobjekte	DPFC				
	Lösch. fremder Sperrobjekte	DLFU				
	Generalberecht. auch fremd. Mandant	* oder ALL				
<b>S_LOG_COM</b> Logische Betriebssystemkommandos		<b>COMMAND</b> <i>SXPGCOSTAB/ SXPGCOTABE</i>	<b>HOST</b>	<b>OPSYSTEM</b>		Nur für System-Admin !
	Generalberecht.	* siehe auch Transaktion SM69	* z.B. Win NT SY-OPSYS	* SY-HOST		
<b>S_NUMBER</b> Nummernkreispflege; Berechtigung zur Verwaltung der Nummernkreise -> Belege, Kred./Deb./Sachk. etc.		<b>ACTVT</b> <i>TACT/TACTZ</i>	<b>NROBJ</b> <i>TNRO/TNRGT</i>			Hierüber kann "hart" in das Systemverhalten eingegriffen werden. Zu beachten: Gesetzl. Rahmenbedingungen. Administrationsobjekt.
	Hinzufügen/Ändern eines Objektes	01/02				
	Nummerkreisstand eines Obj. ändern	11				
	Nummerstände eines Objektes initialisieren	13				
	Nummernkreisobjekt pflegen	17				
	Generalberecht.	*	*			
<b>S_OLE_CALL</b> OLE-Aufruf aus ABAP		<b>ACTVT</b> <i>TACT/TACTZ</i>	<b>OLE_APPL</b>	<b>PROGRAM</b>		Für Admin.
	Ausführen	16				
	Generalberecht.	*	*	*		

S_ADMI_FCD		S_ADMI_FCD				restriktive Vergabe; nur für Basis-Admin
Systemberechtigungen	Netzwerkadministration, z.B. Verwaltung von RFC-Verbindungen	NADM				
	Prozessadministration, z.B. Verwaltung der Benutzer-Modi mit TA SM04	PADM				
	Sperrungen / Entsperrungen von Transaktionen	TLCK				
	Verbuchungsadministration mit TA SM13	UADM				
	Anlegen neuer Mandanten (nur in Kombi. mit S_TABU_DIS und S_TABU_CLI)	T000				
	Mandantenübergreifende Spooladministration, u.a. Einsehen Druckaufträge in allen Mandanten	SPAD + SPAM + SP01				
	Einsehen aller Druckaufträge des eigenen Mandanten (nur in Kombi. mit S_SPO_ACT)	SP01				
	Löschen alter AuditLogs	AUDA				
	Ausführen von UNIX-Befehlen	UNIX				
	Daten löschen ohne Archivierung	RSET				

<b>S_USER_GRP</b>		<b>ACTVT</b> <i>TACT/TACTZ</i>	<b>CLASS</b> <i>USGRP</i>			
Verwaltung von Benutzern	Anlegen von Benutzern	01				
	Ändern von Benutzer inkl. Profizuordnung	02 + 22				
	Löschen von Benutzern	06				
	Kennwörter vergeben und Sperren / Entsperren	05				
	Benutzer SAP* löschen	06	SUPER			
<b>S_USER_AGR</b>		<b>ACTVT</b> <i>TACT/TACTZ</i>	<b>ACT_GROUP</b> <i>AGR_DEFINE/ AGR_AGRS</i>			
Verwaltung von Aktivitätsgruppen	Anlegen neuer AGs	01				
	Ändern von AGs mit Profilgenerierung	02 + 64				
	Benutzer zu AG zuordnen	22				
	ASs löschen	06				
<b>S_USER_PRO</b>		<b>ACTVT</b> <i>TACT/TACTZ</i>	<b>PROFILE</b> <i>USR10</i>			
Verwaltung der Profile	Anlegen neuer Profile	01				
	Ändern von Profilen	02				
	Löschen von Profilen	06				
	Aktivieren von Profilen	07				
<b>S_USER_AUT</b>		<b>ACTVT</b> <i>TACT/TACTZ</i>	<b>AUTH</b> <i>USR12</i>	<b>OBJECT</b> <i>TOBJ</i>		
Verwaltung der Berechtigungen	Anlegen neuer Berechtig.	01				
	Ändern von Berechtig.	02				
	Löschen von Berechtig.	06				
	Aktivieren von Berechtig.	07				

<b>S_USER_OBJ</b> Ausschalten von Berechtigungsobjekten		<b>ACTVT</b> <i>TACT/TACTZ</i>	<b>OBJECT</b> <i>TOBJ</i>			
	Aus/Anschalten von BO	02				
	Aktivieren der Änderungen	07				
<b>S_RZL_ADM</b> Rechenzentrum leitstand		<b>ACTVT</b> <i>TACT/TACTZ</i>				restriktive Vergabe; nur für Basis-Admin
	Systemparameter pflegen, logische BS-Kommandos pflegen	01				
<b>S_SCD0</b> Änderungsbelege verwalten		<b>ACTVT</b> <i>TACT/TACTZ</i>				restriktive Vergabe; nur für Basis-Admins
	Änderungsbelege löschen (ist im Prod.-System nicht zulässig!))	06				
	Änderungsbelegobjekte verwalten	12				
<b>S_TABU_RFC</b> RFC-Datenexport für Mandantenkopien und Vergleiche		<b>ACTVT</b> <i>TACT/TACTZ</i>				restriktive Vergabe; nur für Basis-Admins
	Berechtigung zum Vergleich und Datentransfer	03				
<b>S_SPO_DEV</b> Druckerberechtigungen		<b>SPODEVICE</b> <i>SH_PRIN</i>				
	Drucken auf allen Druckern	*				
<b>S_SPO_ACT</b> Zugriff auf Spool-Aufträge, die geschützt sind durch Berecht.zeich.folgen (fremde Aufträge)	Anz. Inhalt v. geschütztem Auftrag	<b>DISP</b>	<b>SPOAUTH</b>	Eingrenzung auf Gebiet, z.B. FI* o.ä.		
	Ändern von Attributen eines gesch. Auftrags	<b>ATTR</b>		Spool-Admin		
	Ändern eines Berecht.wertes eines gesch. Auftrags	<b>AUTH</b>		nicht zu freigiebig für übliche Nutzer		
	gesch. Auftrag ausgeben 1.Mal	<b>PRNT</b>				
	gesch. Auftrag ausgeben mehrmals	<b>REPR</b>				
	manuelles Löschen	<b>DELE</b>				
	Ändern des Eigentümers	<b>USER</b>				

S_TRANSPRT		ACTVT	TTYPE			
Berechtigung zur Nutzung der Workb., Customizing und des TransportOrg.		TACT/TACTZ				
	Hinzufügen/ Erzeugen / Ändern	01/02	DLOG TASK	lok, Änd.auftr. Aufgaben (Korr., Repar.)		
	Sperren/Lösch.	05/06	DTRA	transport.bare Änder.auftr.		
	Freigeben	43	CUST	Custom.auftr.		
	Quellmandant eines Auftrags ändern	50	TRAN	Transporte v. Kopien		
	Import	60	CLCP	Mandanten- transporte		
	Freig. fremd. Aufträge	75				
	Generalberecht.	*				

## 5. Fazit und weiteres Vorgehen

Das SAP R/3-Berechtigungsumfeld ist ein umfangreiches und für den Revisor ergiebiges Gebiet, das - aufgeteilt in unterschiedliche Prüfungsschwerpunkte - mehrmals jährlich einer Prüfung unterzogen werden sollte. Die zuständigen Fachbereiche (SAP-Basis, Finanzbereich etc.) müssen jedoch auch angehalten werden, regelmäßig mit den eigenen Prüfungsschwerpunkten Reviews durchzuführen, um im Eigeninteresse Transparenz über die zugrundeliegenden Berechtigungen zu erhalten. Im Zuge der Vor- und Nachbereitung von Berechtigungsprüfungen ist bei der Vielzahl von Prüfobjekten in SAP R/3 eine Dokumentation wie hier vorliegend sinnvoll. Als Ergebnis sollten vorhandene Profile um die entsprechenden Berechtigungsobjekte und Einzelausprägungen, - insbesondere mit Generalfunktionalität - korrigiert werden, besonders auch die der Basis- und Modul-Administration.

Die Fortsetzung dieses Artikels wird sich auf gleiche Weise mit den Berechtigungsobjekten der Module FI und CO beschäftigen. Gerade auch in diesen Bereichen werden oftmals umfangreiche Berechtigungen zur Debitoren-, Kreditoren-, Sach- und Anlagenverwaltung vergeben, aus denen nicht unerhebliches Gefahrenpotenzial resultiert.

01	Hinzufügen/Erzeugen	40	Anlegen auf Datenbank
02	Ändern	41	Löschen auf Datenbank
03	Anzeigen	42	Umsetzen auf Datenbank
04	Drucken	60	Importieren
05	Sperren	61	Exportieren
06	Löschen	63	Aktivieren
07	Aktivieren/Generieren	64	Generieren
08	Änderungsbelege anzeigen	65	Reorganisieren
10	Buchen	66	Aktualisieren
16	Ausführen	70	Verwalten, Administrieren
21	Transportieren	71	Auswerten
22	Eintragen, Aufnehmen, Zuordnen	85	Stornieren
23	Pflegen	91	Reaktivieren
24	Archivieren	A1	Rückstellen
27	Summensätze anzeigen	A2	Auszahlen
28	Einzelposten anzeigen	A3	Status ändern
29	Gespeicherte Daten anzeigen	A5	Berichte anzeigen
33	Lesen	A6	Lesen mit Filter

Tabelle: Auszug aus der Aktivitätenliste

**Ausgesuchte Literatur :**

SAPaudit	Fa. ibs schreiber gmbh, Hamburg / RevCon revision und consulting GmbH, Hannover	
Thomas Tiede	SAP R/3 Ordnungsmäßigkeit und Prüfung des SAP-Systems	2000
Uwe Bernd-Striebeck/ Thomas Glauch u.a.	SAP R/3 Sicherheit und Prüfung	1998
Paul Wenzel	Betriebswirtschaftliche Anwendungen des integrierten Systems SAP R/3	1995
Horst Keller / Sascha Krüger	ABAP Objects	2001
Rüdiger Kretschmer / Wolfgang Weiss	SAP R/3 - Entwicklung mit ABAP/4	1999

Mit besonderem Dank an Thomas Tiede, Fa. ibs schreiber gmbh, Hamburg, Technischer Geschäftsführer und Leiter Qualitätsmanagement und Prüfungen, für die freundliche Unterstützung.

**Ergänzungen zur einzelnen Berechtigungsobjekten – kritische Eingrenzungen:**

S\_USER\_AUT und S\_USER\_PRO

Feld ACTVT ,Aktivität': 22 Profil Benutzern zuordnen  
24 Archivieren

S\_USER\_OBJ

Feld ACTVT ,Aktivität': 21 Aufnehmen in Transportauftrag

S\_USER\_SYS

Feld AKTVT ,Aktivität': 02 Ändern  
68 Benutzer und Aktivitätsgruppen modellhaft zuordnen  
78 System einem Benutzer zuordnen, so dass er in das System verteilt wird  
90 Initiale Übernahme von Benutzern aus dem System

S\_USER\_WWW

Feld ACTVT ,Aktivität': 01 Hinzufügen / Erzeugen  
02 Ändern  
05 Sperren  
06 Löschen  
23 Passwort pflegen  
45 Erlauben  
51 Initialisieren  
90 Übernehmen

S\_USER\_AGR

Feld ACTVT ,Aktivität': 21 Transportieren von Aktivitätsgruppen  
68 Modellieren  
78 Zuordnen im Zentralsystem bei zentr. Benutzeradmin. zu Systemen oder Benutzergruppen  
DL Download  
UP Upload

siehe SAP PRESS: SAP Berechtigungswesen – Design und Realisierung von Berechtigungskonzepten für SAP R/3 und SAP Enterprise Portal (Beyer/Fischer/Probst u.a.), 2003, S.285ff