



Marcel Schmiechen

Berechtigungen im SAP® ERP HCM – Einrichtung und Konfiguration

- ▶ Rollen- und Profilvergabe im SAP-Personalwesen
- ▶ strukturelle und kontextsensitive Berechtigungen
- ▶ Aufbau eines HCM-Berechtigungskonzepts
- ▶ SAP-Portalrollen vs. Backend-Rollen

Inhaltsverzeichnis

Einleitung	9
1 Einführung in das HCM-Berechtigungswesen	11
1.1 Beispiele für Infotypen	12
1.2 Berechtigungsfelder	15
2 Berechtigungen der HCM-Komponenten	21
2.1 Personaladministration	21
2.2 Zeitwirtschaft	22
2.3 Organisationsmanagement	22
2.4 E-Recruiting	24
2.5 Learning Solution	26
2.6 Stellenwirtschaft	26
2.7 Personalentwicklung	27
2.8 Abrechnung	27
3 Aufbau eines HCM-Berechtigungskonzepts	29
3.1 Erhebung der Anforderungen der Fachteams	32
3.2 HR-Berechtigungshauptschalter	46
3.3 Toleranzzeit der Berechtigungsprüfung	55
3.4 Vier-Augen-Prinzip	56
3.5 Eigene Berechtigungsobjekte anlegen	59
4 Strukturelle Berechtigungen	71
4.1 Konfiguration struktureller Berechtigungen	72
4.2 Zuweisung struktureller Berechtigungen	74
4.3 Exkludieren struktureller Profile	76
4.4 Exkurs Auswertungswege	77

4.5	Kontextsensitive Berechtigungen	81
4.6	Pufferung von strukturellen Berechtigungen	87
5	Berechtigungen im SAP Enterprise Portal	95
5.1	Technische Grundlagen	96
5.2	Portal-Objekte	100
5.3	Benutzerverwaltung	104
5.4	Rollen im Portal	106
5.5	UME-Aktionen	110
5.6	UME-Gruppen	111
5.7	Zuweisung portalseitiger Rollen im Backend	116
6	Benutzeradministration	117
6.1	Die HR-Berechtigungs-Workbench	117
6.2	Benutzerpflege in der Transaktion SU01	121
6.3	Pflege der Tabelle T77UA	122
6.4	Pflege des Infotyps 0105 – Subtyp 0001	123
7	Datenschutz	125
7.1	Prinzipien des Datenschutzes	125
7.2	Rollen für den Datenschutzbeauftragten	128
8	Fehlersuche	131
8.1	Transaktion SU53	131
8.2	Transaktion STAUTHTRACE	134
8.3	Report RH_AUTH_CUST_CHECK	146
8.4	Debugging	149
9	Erweiterung der Berechtigungssteuerung	151
9.1	BAdI HRPAD00AUTH_CHECK	151
9.2	BAdI HRPAD00AUTH_TIME	154

9.3	BAdI HRBAS00_STRUAUTH	155
9.4	BAdI HRBAS00_GET_PROFL	156
10	Fazit	161
A	Der Autor	164
B	Index	165
C	Disclaimer	169
	Weitere Bücher von Espresso Tutorials	170

2 Berechtigungen der HCM-Komponenten

Wenden wir uns nun den einzelnen Komponenten des Moduls HCM zu und betrachten wir, in welchen Besonderheiten und Merkmalen sich diese voneinander unterscheiden.

Die einzelnen HCM-Komponenten verwenden teils unterschiedliche Funktionen und Verfahren der Berechtigungssteuerung. So kommen zum einen allgemeine Berechtigungsprüfungen und Vergaben zum Einsatz, die auch aus anderen SAP-Modulen bekannt sind, zum anderen aber auch solche, die exklusiv dem HCM vorbehalten sind wie z. B. strukturelle Berechtigungen (siehe Kapitel 4).

2.1 Personaladministration

Die Personaladministration bzw. deren Stammdaten sind elementare Bestandteile und Voraussetzung zur Nutzung der meisten Geschäftsprozesse und Funktionen im SAP HCM, da hier die Stammdaten der Personalfälle vorgehalten werden.

Die Berechtigungssteuerung für den Zugriff auf Infotypen der Personaladministration erfolgt über die Berechtigungsobjekte

- ▶ P_ORGIN (siehe Abschnitt 3.2.7) und
- ▶ P_ORGXX (siehe Abschnitt 3.2.9)

oder beim Einsatz der kontextsensitiven Berechtigungen (eine nähere Erläuterung folgt in Abschnitt 4.5) über

- ▶ P_ORGINCON (siehe Abschnitt 3.2.4) und
- ▶ P_ORGXXCON (siehe Abschnitt 3.2.11).

Der Zugriff auf die Infotypen der Personaladministration im Rahmen von ESS-Szenarien (Employee Self Services) wird über das Berechtigungsobjekt P_PERNR (siehe Abschnitt 3.2.10) gesteuert.

Darüber hinaus können zusätzlich strukturelle Berechtigungen zum Einsatz kommen.

2.2 Zeitwirtschaft

Die Zugriffssteuerung im Bereich der Zeitwirtschaft wird sehr unterschiedlich gehandhabt. Bei vielen Projekten erfolgt die Berechtigungsvergabe über die identischen Berechtigungsfelder (und somit auch Berechtigungsobjekte) wie in der Personaladministration. Je nach Unternehmensstruktur kann es aber auch vorkommen, dass die Steuerung über das für den Bereich Zeitwirtschaft zur Verfügung stehende *Sachbearbeiterkennzeichen* geschieht.

Die Sachbearbeiterkennzeichen für das HCM sind in den Berechtigungsobjekten

- ▶ P_ORGXX und
- ▶ P_ORGXXCON

enthalten. Des Weiteren können auch in der Zeitwirtschaft zusätzlich *strukturelle Berechtigungen* zum Einsatz kommen.

Dagegen finden die außerdem im HCM vorhandenen Sachbearbeiterkennzeichen für Personal und Abrechnung selten zur Steuerung von Berechtigungen Verwendung.

2.3 Organisationsmanagement

Das *Organisationsmanagement* arbeitet für den Zugriff auf die Daten in den *PD-Infotypen* (Planung) mit dem Berechtigungsobjekt PLOG (siehe Abbildung 2.1) und der Vergabe struktureller Berechtigungen (siehe Kapitel 4).

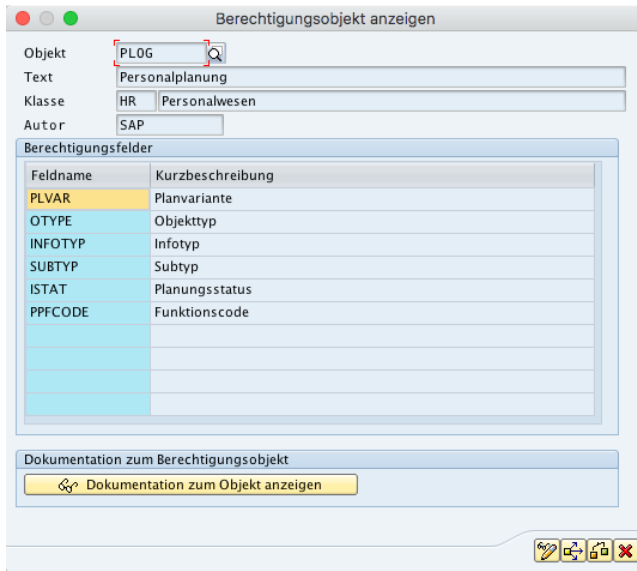


Abbildung 2.1: Berechtigungsobjekt PLOG

Das Berechtigungsobjekt hat mittels der darin enthaltenen Felder die Möglichkeit der Aussteuerung des Zugriffs auf

- ▶ eine Planvariante (vgl. Abschnitt 1.2.6),
- ▶ einen Objektyp (Feld OTYPE) wie z. B. Organisationseinheit, Planstellen und Personen,
- ▶ Infotypen (Feld INFOTYP),
- ▶ den Subtyp (Feld SUBTYP),
- ▶ den Planungsstatus (Feld ISTAT) und
- ▶ das Feld PFFCODE (Funktionscode), das die Art des Zugriffs bestimmt.

Dies sind alle Elemente und Informationen, die für Infotypen der Planung (PD-Infotypen) relevant sind.

Die möglichen Werte für den Funktionscode sind in der Tabelle T77FC abgelegt (Abbildung 2.2).

Data Browser: Tabelle T77FC 33 Treffer

Tabelle: T77FC
 Angezeigte Felder: 11 von 11 Feststehende Führungsspalten: Listbreite 0250

MANDT	FPCODE	PSTAT	FSTA1	FSTA2	ENQUE	MODGR	MAINT	DIDENT	LFCOD	FTEXT
<input type="checkbox"/>	001	INIT	00	00		1		0000		
<input type="checkbox"/>	001	ABLN	MODI	00	01	1	X	0000	ABLN	Ablehnen
<input type="checkbox"/>	001	AEND	MODI	00	04	1	X	0000		Ändern
<input type="checkbox"/>	001	AENK	MODK	00	04	1		0000		Kantinenfeld ändern
<input type="checkbox"/>	001	AENT	MODT	00	08	1		0000		Temporär ändern
<input type="checkbox"/>	001	AKTI	BEAN	00	01	1	X	0000	AKTI	Aktivieren
<input type="checkbox"/>	001	BEAN	BEAN	00	01	1	X	0000	BEAN	Beantragen
<input type="checkbox"/>	001	COP	MODI	00	04	1	X	0000		Kopieren
<input type="checkbox"/>	001	COPR	COPY	00	04	1		0000		Raum kopieren
<input type="checkbox"/>	001	COPY	COPY	00	04	1		0000		Objekt kopieren
<input type="checkbox"/>	001	CUT	CUT	00	08	1	X	0000	CUT	Objekt abgrenzen
<input type="checkbox"/>	001	CUTI	CUTI	00	01	1	X	0000	CUTI	Abgrenzen
<input type="checkbox"/>	001	DEL	DEL	00	02	1	X	0000		Löschen
<input type="checkbox"/>	001	DELO	DELO	00	02	1	X	0000	DELO	Objekt löschen
<input type="checkbox"/>	001	DISP	DISP	00	01	1		0000		Anzeigen
<input type="checkbox"/>	001	DUTY	INOQ	00	08	1	X	0000		Mußverknüpfung
<input type="checkbox"/>	001	GENE	BEAN	00	01	1	X	0000	GENE	Genehmigen
<input type="checkbox"/>	001	HITK	HITK	00	01	1		0000		Hittliste Karriereplanung
<input type="checkbox"/>	001	HITS	HITS	00	08	1		0000		Karriereplan Simulation
<input type="checkbox"/>	001	HITW	HITW	00	01	1		0000		Hittl. Weiterbildungsplan
<input type="checkbox"/>	001	INIT	INIT	00	00	1		0000		Initialisierung
<input type="checkbox"/>	001	INSE	INSE	00	08	1	X	0000		Anlegen
<input type="checkbox"/>	001	INSG	GMOD	00	08	1	X	0000		Anlegen aus 05/2
<input type="checkbox"/>	001	INTE	INTE	00	08	2		0000		Integration
<input type="checkbox"/>	001	LISD	LISD	00	00	1		0000		Listanzeige
<input type="checkbox"/>	001	LIST	LIST	00	00	1	X	0000		Listanzeige mit Änderung
<input type="checkbox"/>	001	MASS	INOQ	00	08	1	X	0000		Anlegen
<input type="checkbox"/>	001	NEWL	MODI	00	00	1		0000		Neue Sprache
<input type="checkbox"/>	001	PLVG	GMOD	00	00	1	X	0000		Planvorsch. aus 05/2
<input type="checkbox"/>	001	PLVO	MODI	00	00	1	X	0000	PLVO	Planvorschlägen
<input type="checkbox"/>	001	QUIC	QUIC	00	08	1	X	0000		Schnellerfassung
<input type="checkbox"/>	001	SIMU	HITS	00	08	1		0000		Simulation
<input type="checkbox"/>	001	VORS	VORS	00	08	1		0000		Vorselekt. Nachfolgeplan

Abbildung 2.2: Mögliche Werte im Berechtigungsfeld PFFCODE

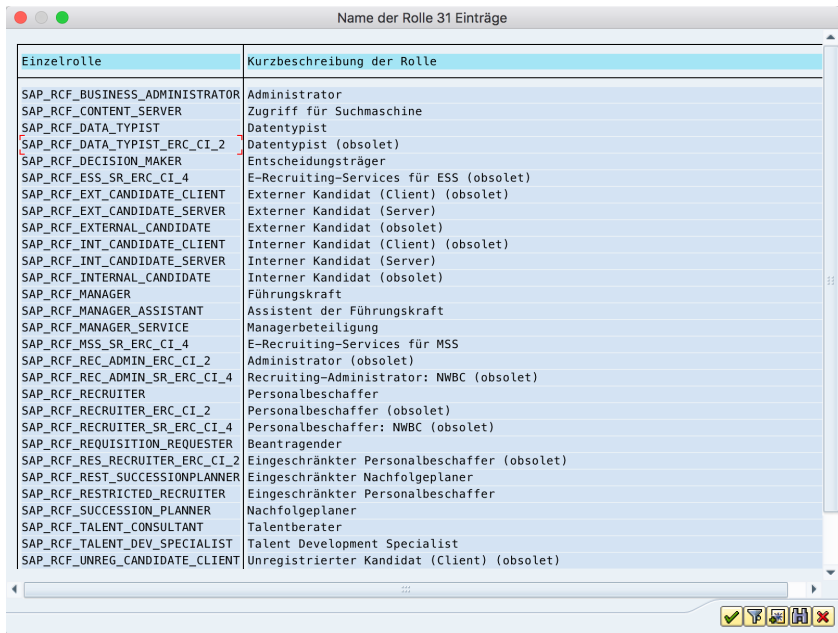
In der Regel werden außerdem einige Personalstammdaten benötigt, um z.B. die Namen der Mitarbeiter innerhalb des Organisationsmanagements anzuzeigen. Dazu werden die Berechtigungsobjekte analog zur Personaladministration in den Rollen benötigt. Dies bedeutet, dass etwa in die Rollen für das Organisationsmanagement ebenfalls Berechtigungsobjekte der Personaladministration aufgenommen werden müssen.

2.4 E-Recruiting

Das *E-Recruiting* ist i.d.R. nicht auf dem SAP-HCM-System integriert, sondern wird aus Sicherheitsgründen auf einem gesonderten System betrieben. Dieses ist den meisten Fällen zusätzlich in ein Front- und ein Backend-System aufgeteilt. Das Frontend-System steht vor allem für einen externen Zugriff aus dem Internet zur Verfügung, etwa für Bewerber auf eine ausgeschriebene Stelle im Unter-

nehmen. Es kommuniziert über das Backend-System, das in einer gesicherten Netzwerkzone mit dem eigentlichen HCM-System in Verbindung steht.

Die Berechtigungssteuerung im Bereich E-Recruiting unterscheidet sich aufgrund dieser strukturellen Gegebenheit von den übrigen Komponenten im SAP HCM, bei denen i. d. R. von einer Verwendung der SAP-Standard-Rollen als Grundlage für die Erstellung spezifischer Rollen zum Projekt abzusehen ist. Im E-Recruiting kann es durchaus sinnvoll sein, sich die im SAP-Standard ausgelieferten Rollen anzuschauen und teilweise direkt zu verwenden. So ist davon auszugehen, dass sich der Zugriff und die Berechtigungen für einen externen oder internen Bewerber kaum von den ausgelieferten Standard-Rollen unterscheiden, da diese Funktionen in den Unternehmen nur sehr geringfügig voneinander abweichen. Die Standard-Rollen beginnen mit dem Präfix `SAP_RCF*`. Abbildung 2.3 zeigt die mit Release 7.50 ausgelieferten Rollen.



Einzelrolle	Kurzbeschreibung der Rolle
SAP_RCF_BUSINESS_ADMINISTRATOR	Administrator
SAP_RCF_CONTENT_SERVER	Zugriff für Suchmaschine
SAP_RCF_DATA_TYPIST	Datentypist
SAP_RCF_DATA_TYPIST_ERC_CI_2	Datentypist (obsolet)
SAP_RCF_DECISION_MAKER	Entscheidungsträger
SAP_RCF_ESS_SR_ERC_CI_4	E-Recruiting-Services für ESS (obsolet)
SAP_RCF_EXT_CANDIDATE_CLIENT	Externer Kandidat (Client) (obsolet)
SAP_RCF_EXT_CANDIDATE_SERVER	Externer Kandidat (Server)
SAP_RCF_EXTERNAL_CANDIDATE	Externer Kandidat (obsolet)
SAP_RCF_INT_CANDIDATE_CLIENT	Interner Kandidat (Client) (obsolet)
SAP_RCF_INT_CANDIDATE_SERVER	Interner Kandidat (Server)
SAP_RCF_INTERNAL_CANDIDATE	Interner Kandidat (obsolet)
SAP_RCF_MANAGER	Führungskraft
SAP_RCF_MANAGER_ASSISTANT	Assistent der Führungskraft
SAP_RCF_MANAGER_SERVICE	Managerbeteiligung
SAP_RCF_MSS_SR_ERC_CI_4	E-Recruiting-Services für MSS
SAP_RCF_REC_ADMIN_ERC_CI_2	Administrator (obsolet)
SAP_RCF_REC_ADMIN_SR_ERC_CI_4	Recruiting-Administrator: NWBC (obsolet)
SAP_RCF_RECRUITER	Personalbeschaffer
SAP_RCF_RECRUITER_ERC_CI_2	Personalbeschaffer (obsolet)
SAP_RCF_RECRUITER_SR_ERC_CI_4	Personalbeschaffer: NWBC (obsolet)
SAP_RCF_REQUISITION_REQUESTER	Beantragender
SAP_RCF_RES_RECRUITER_ERC_CI_2	Eingeschränkter Personalbeschaffer (obsolet)
SAP_RCF_REST_SUCCESSIONPLANNER	Eingeschränkter Nachfolgeplaner
SAP_RCF_RESTRICTED_RECRUITER	Eingeschränkter Personalbeschaffer
SAP_RCF_SUCCESSION_PLANNER	Nachfolgeplaner
SAP_RCF_TALENT_CONSULTANT	Talentberater
SAP_RCF_TALENT_DEV_SPECIALIST	Talent Development Specialist
SAP_RCF_UNREG_CANDIDATE_CLIENT	Unregistrierter Kandidat (Client) (obsolet)

Abbildung 2.3: SAP-Standard-Rollen E-Recruiting

B Index

A

abgeleitete Rolle 39
 Abrechnung 27
 Auswertungsweg 73, 77, 79

B

BAdI 76, 151
 HRBAS00_GET_PROFL 76, 86,
 156
 HRBAS00_STRUAUTH 155
 HRPAD00AUTH_CHECK 149,
 151
 HRPAD00AUTH_TIME 154
 Benutzer 11
 SAP* 118
 Benutzerantrag 32
 Benutzerpuffer 19
 SU56 19
 Benutzerstammsatz 13
 Berechtigungsfeld 14, 15, 41, 44
 AUTHC 19
 Sachbearbeiter Abrechnung 18
 Sachbearbeiter Personalstamm
 18
 Sachbearbeiter Zeiterfassung 18,
 22
 Berechtigungskonzept 29, 30
 Berechtigungslevel 148
 Berechtigungsobjekt 14
 P_NNNNNCON 62, 65
 P_ORGIN 16, 17, 21, 51

P_ORGINCON 16, 17, 19, 21,
 49, 83, 84
 P_ORGXX 18, 21, 22, 51, 54, 85
 P_ORGXXCON 18, 19, 21, 22,
 54, 83, 85
 P_PERNR 22, 123, 148
 PLOG 86
 PLOG_CON 86

Berechtigungsprüfung 13, 15
 Berechtigungssteuerung 29
 Berechtigungstrace 139
 betriebswirtschaftliche Rolle 34

C

CL_HRPAD00AUTH_CHECK_
 STD 154

D

Datenschutz 125
 Debugging 149
 CL_HRPAD00AUTH_CHECK_
 FAST 149
 CL_HRPAD00AUTH_CHECK_
 STD 149
 Deltalink 101
 Domäne 16

E

E-Recruiting 24
 ESS 14, 22, 53, 74, 95
 exkludieren 76

F

Fehlersuche 131
Funktionsbaustein 74
RH_AUTHORITY_CHECK_
FROM_ADMIN 150
RH_AUTHORITY_CHECK_
ORGEH 150
RH_BASE_AUTHORITY_CHECK
150
RH_GET_MANAGER_
ASSIGNMENT 74
RH_GET_ORG_ASSIGNMENT
74
RH_STRU_AUTHORITY_CHECK
150
RH_STRU_AUTHORITY_CHECK
_PP01 150

Funktionscode 23
Funktionstrennung 34
Funktionstrennungsprinzip 125,
126

G

Genehmigungsprinzip 125, 127
generische Rolle 38

H

HRAUTH Siehe HR-
Berechtigungs-Workbench
HR-Berechtigungs-Hauptschalter
35, 46, 117
ADAYS 48
APPRO 48
DFCON 49
INCON 49
NNCON 49
NNNNN 50
ORGIN 50

ORGPD 51
ORGXX 51
PERNR 52
XXCON 54

HR-Berechtigungs-Workbench
117

I

Identitätsprinzip 125, 126
Identitätsverwaltung 104, 114
Infotyp 12
iView 100, 108

J

J2EE-Sicherheitsrolle 100, 106,
109

K

Kontextprüfung 49
kontextsensitive Berechtigung
81
Kontrollprinzip 126, 127
kundeneigenes
Berechtigungsobjekt 19, 49,
59

L

LDAP 97
Learning Solution 26

M

Minimalprinzip 125, 126
Mitarbeitergruppe 16, 17
MPPAUTCON 67
MSS 14, 53, 74, 95

O

OOAC 47
 OOSB 74, 76, 118, 122
 OOSP 71, 72
 Organisationsmanagement 22
 Organisationsschlüssel 18
 Orgebene 31, 40, 42, 46
 Orgebenefeld 40

P

P_PERNR 52
 Permissions 106
 Personaladministration 21
 Personalbereich 16, 39
 Personalentwicklung 27
 PFCG 16, 40
 Planstelle 49
 Planvariante 19, 23
 PLOG 19, 22, 26, 27
 Portal 14, 53
 Gruppe 102
 Seite 101
 Portal Content Directory 103
 Portalrolle 95, 107
 Profil 14
 Prüfverfahren 48
 Pufferung 87
 RHBAUS_PARALLEL 88, 89, 90
 RHBAUS00 90
 RHBAUS01 89, 90
 RHBAUS02 89

R

Report
 PFCG_ORGFIELD_CREATE 43
 PFCG_ORGFIELD_DELETE 45

PFCG_ORGFIELD_UPGRADE
 46
 RH_AUTH_CUST_CHECK 131,
 146
 RPUACG00 65

Rolle 13
 Rollenkonzept 31, 32, 35
 Rollenmatrix 35
 Rollenmenü 32

S

Schriftformprinzip 126, 127
 Schwellwert 91
 Sperrkennzeichen 57
 ST01 134
 Standardprinzip 126, 127
 STAUTHTRACE 131, 134
 Stellenwirtschaft 26
 strukturelle Berechtigung 22, 27,
 71, 82, 87, 131
 strukturelles Profil 19, 34, 71,
 75, 80
 SU20 16
 SU21 61, 141
 SU53 131
 Systemtrace 134

T

Toleranzzeit 55

U

UME
 -Aktion 100, 108, 110
 -Gruppe 100, 111, 116
 -Rolle 100, 106, 108, 112, 114,
 116

User Management Engine
(UME) 96, 98, 104
User Persistence Store 96

V

Veranstaltungsmanagement 26
Vier-Augen-Prinzip 56
 asymmetrisch 57
 symmetrisch 56

W

Workset 101, 108
Worksets 101

Z

Zeitwirtschaft 22
Zugangsschlüssel 63
Zugriffskontrollliste 100
Zuständigkeitsbereich 39