

Inhaltsverzeichnis

Vorwort	9
1 Neuerungen: Technische Durchführung einer Berechtigungsprüfung	13
1.1 Berechtigungsprüfungen in Core Data Services	13
1.2 Berechtigungsprüfungen im ALV Grid	22
2 SAP Business User	25
2.1 SAP-Benutzerstammsatz versus Business User	25
2.2 Mitarbeiter und Geschäftspartner zuordnen (ohne HR-Integration)	28
2.3 Mitarbeiter und Geschäftspartner zuordnen (mit HR-Integration)	34
3 Fiori-Rollen	39
3.1 Grundbegriffe	39
3.2 Berechtigungsrelevante Informationen zu einer App bestimmen	44
3.3 Fiori-Frontend-Rolle definieren	60
3.4 Berechtigungen im Backend- und im Frontend-System	66
4 Spezielle Berechtigungen für das Launchpad	71
4.1 SAP-Standardrollen für das Fiori Launchpad	71
4.2 Personalisierung deaktivieren	72
4.3 Berechtigungen für die Enterprise Search	74
5 Profilgenerator: Fiori-spezifische Installations- und Upgradearbeiten	81
5.1 Aktualisierung von Fiori-Frontend-Rollen	81
5.2 Vorschlagswerte für Fiori-Apps	83
6 Definition eigener Berechtigungsobjekte	87
6.1 Objektklasse anlegen	87
6.2 Berechtigungsobjekt anlegen	88
6.3 Fallbeispiel: Kostenstellenstammsatz	91
	5

7	Berechtigungszuordnung über Organisationseinheiten	109
7.1	Beispiel für ein Organisationsmodell	109
7.2	Definition der Beispielrollen	110
7.3	Zuordnung einer Rolle zur Organisationseinheit	113
7.4	Zuordnung von Rollen zu Stellen und Planstellen	117
7.5	Anzeige der Zuordnungen in SU01	119
7.6	Änderung der Organisationsstruktur	120
8	Funktionstrennung (SOD)	123
8.1	Grundbegriffe	123
8.2	Transaktion für Definition und Auswertungen	126
8.3	Definition einer kritischen Berechtigung	127
8.4	Auswertung einer kritischen Berechtigung	130
8.5	SAP-Muster für kritische Berechtigungen	132
8.6	Kritische Kombination von Berechtigungen	133
8.7	Auswertung kritischer Kombinationen	136
8.8	Download und Upload von kritischen Berechtigungen	138
9	Zentrale Benutzerverwaltung	143
9.1	Beispielkonstellation	143
9.2	Einrichtung der ZBV – Teil 1	145
9.3	Einrichtung der ZBV – Teil 2	153
9.4	Benutzer im ZBV-Zentralsystem anlegen	165
9.5	Verteilungsprotokoll auswerten	169
9.6	Benutzerpflege im Tochtersystem	170
9.7	Fehleranalyse	172
9.8	Hintergrundinformationen zur ZBV	177
9.9	ZBV auflösen	183
9.10	Check und Monitoring der ZBV	186
10	Berechtigungskonzept für SAP-J2EE-Systeme	189
10.1	Grundbegriffe	189
10.2	UME-Konsole	192
10.3	UME-Rolle anlegen	198
10.4	ABAP-System als Datenquelle	201

10.5	Log-in-Vorgang bei Datenquelle »ABAP-System«	210
10.6	Analyse von Berechtigungsfehlern	212
11	Relevante System-Profilparameter/Customizing-Schalter	219
11.1	System-Profilparameter	219
11.2	Ausnahmeliste für Kennworte	225
11.3	Customizing Benutzermenü SAP Easy Access/ Rollenpflege	226
11.4	Konfiguration des Fiori Launchpad	229
12	Definition von Sicherheitsrichtlinien	231
12.1	Grundbegriffe Sicherheitsrichtlinien	231
12.2	Sicherheitsrichtlinie anlegen	231
12.3	Sicherheitsrichtlinie prüfen	233
12.4	Änderungshistorie für Sicherheitsrichtlinien	234
12.5	Sicherheitsrichtlinie zuweisen	235
13	Archivierung von berechtigungsrelevanten Daten	237
13.1	Informationen zur Archivierung	237
13.2	Änderungsbelege für Benutzer (US_PASS)	240
13.3	Übrige Änderungsbelege archivieren	244
13.4	Auswertung der archivierten Belege	246
14	Security-Audit-Log	249
14.1	Grundlagen des Security-Audit-Log	249
14.2	Relevante Transaktionen	251
14.3	Konfiguration des Audit-Log	252
14.4	Security-Audit-Log auswerten	264
14.5	Logdateien und Logtabelle reorganisieren	266
15	Fazit	269
A	Der Autor	271
B	Index	273
C	Disclaimer	276