

## Leseprobe

In dieser Leseprobe erfahren Sie, wie Sie ein ausdifferenziertes und effizientes Berechtigungskonzept entwickeln. Die Autoren zeigen Ihnen, welche Einstellungen und Funktionen Ihnen die Berechtigungspflege erleichtern und stellen Ihnen unterschiedliche Tracemöglichkeiten vor. Außerdem wissen Sie nach der Lektüre, wie Sie nach einem Upgrade die Rollen und Berechtigungen überführen und erhalten Tipps zu den Parametern für Kennwortregeln.



**Systemeinstellungen und Customizing:  
»Pflege und Nutzung der Vorschläge für den  
Profilgenerator«**

**»Traces«**

**»Upgrade-Nacharbeiten von Berechtigungen«**

**»Parameter für Kennwortregeln«**



**Inhaltsverzeichnis**



**Index**



**Die Autoren**



**Leseprobe weiterempfehlen**

Volker Lehnert, Katharina Stelzner, Anna Otto, Peter John

### **SAP-Berechtigungswesen – Konzeption und Realisierung**

847 Seiten, gebunden, 3. Auflage 2016  
79,90 Euro, ISBN 978-3-8362-3768-0



[www.sap-press.de/3849](http://www.sap-press.de/3849)



*Dieses Kapitel beschreibt die Einstellungen und Funktionen in der Rollen- und Berechtigungsadministration. Diese ermöglichen ein ausdifferenziertes Berechtigungskonzept und erleichtern Ihnen die Pflege der Berechtigungen.*

## **7 Systemeinstellungen und Customizing**

Der Aufbau dieses Kapitels folgt dem normativen Ansatz der Berechtigungspflege. Normativ ist der Ansatz, weil das Ziel der Regelkonformität (siehe Kapitel 4, »Rechtlicher Rahmen – normativer Rahmen«) nur durch möglichst präzise Regeln erreichbar ist. Aus den gesetzlichen Regeln müssen Regeln der Organisation werden. Aus diesen müssen wiederum für das Berechtigungskonzept technische Regeln werden. Die wichtigste technische Regel besteht darin, dass die Möglichkeiten des technischen Systems effizient genutzt und nicht umgangen werden.

Entsprechend ist Abschnitt 7.1, »Pflege und Nutzung der Vorschläge für den Profilgenerator«, den Berechtigungsvorschlagswerten gewidmet, die eine effiziente Pflege von Rollen erst ermöglichen. In Abschnitt 7.2, »Traces«, stellen wir die unterschiedlichen Tracemöglichkeiten vor. Abschnitt 7.3 beschreibt die Upgrade-Nacharbeiten von Berechtigungen. Wir beziehen uns in diesem Abschnitt systematisch auf die Tätigkeiten nach einem Upgrade im Bezug auf den Profilgenerator und somit auf die Überführung der Rollen, gestützt auf die Berechtigungsvorschlagswerte. Abschnitt 7.4 stellt schließlich »Parameter für Kennwortregeln« vor.

In Verbindung mit Kapitel 6, »Technische Grundlagen der Berechtigungspflege«, werden Sie mit diesen Abschnitten alle Einstellungen für den Betrieb eines normativ fundierten Berechtigungskonzepts kennengelernt und erfahren haben, welcher Zusammenhang zwischen den Möglichkeiten im SAP-System und den Anforderungen an die Regelkonformität besteht.

Die nächsten Abschnitte stellen wichtige Erweiterungen des Berechtigungskonzepts dar, die es Ihnen ermöglichen, Regelkonformität zu erreichen: Abschnitt 7.5, »Menükonzept«, beschreibt die Möglichkeiten eines normativen Menükonzepts, und Abschnitt 7.6 führt Sie in die Nutzung und Erweiterung von Berechtigungsgruppen in Bezug auf optionale Prüfungen und die Tabellenberechtigungen ein. In Abschnitt 7.7, »Parameter- und Query-Transaktionen«, erfahren Sie, wie Sie Tabellenzugriffe und Querys in Transaktionen umwandeln können, um zu verhindern, dass Endbenutzer direkte Tabellenzugriffe haben.

Um die Möglichkeiten, ein Standardberechtigungskonzept zu erstellen, auszuprägen und kundenspezifische Einstellungen, Transaktionen und Funktionen zu ergänzen, folgen die nächsten drei Abschnitte: Abschnitt 7.8, »Anhebung eines Berechtigungsfeldes zur Organisationsebene«, widmet sich der weiteren organisatorischen Differenzierung Ihres Berechtigungskonzepts mittels zusätzlicher Organisationsebenen. Abschnitt 7.9, »Berechtigungsfelder und -objekte anlegen«, beschreibt die Anlage eigener Berechtigungsobjekte. Abschnitt 7.10, »Weitere Transaktionen der Berechtigungsadministration«, stellt eine Sammlung weiterer nützlicher Transaktionen vor. Zusätzlich sollten Sie im Rahmen der Ermittlung von erforderlichen Berechtigungen vor allem in kundeneigenen Programmen die Informationen in Abschnitt 7.2, »Traces«, berücksichtigen.

## 7.1 Pflege und Nutzung der Vorschläge für den Profilgenerator

In diesem Abschnitt stellen wir die zentrale Funktion der Berechtigungsvorschlagswerte dar. Berechtigungsvorschläge sind vordefinierte Werte, die beim Anlegen und Ändern von Rollen auf Basis des Rollenmenüs als Berechtigungen vorgeschlagen werden. Sie erleichtern die effiziente und regelkonforme Pflege von Rollen.

Bedeutung der Vorschlagswerte

Abbildung 7.1 verdeutlicht die zentrale Bedeutung der Pflege der Berechtigungsvorschlagswerte sowohl für alle Aktivitäten der Rollenpflege als auch für alle analytischen Methoden. Im mittleren Bereich der Abbildung sehen Sie, dass für jede Anwendung (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) Berechtigungsvorschläge festgelegt werden. Diese Berechtigungsvor-

schläge können dann in der Rollenpflege übernommen werden. Darüber hinaus werden die Berechtigungsvorschlagswerte für die Risikoanalyse (kritische Aktionen, Funktionstrennungskonflikte) und die technische Analyse (Normeinhaltung) benötigt.

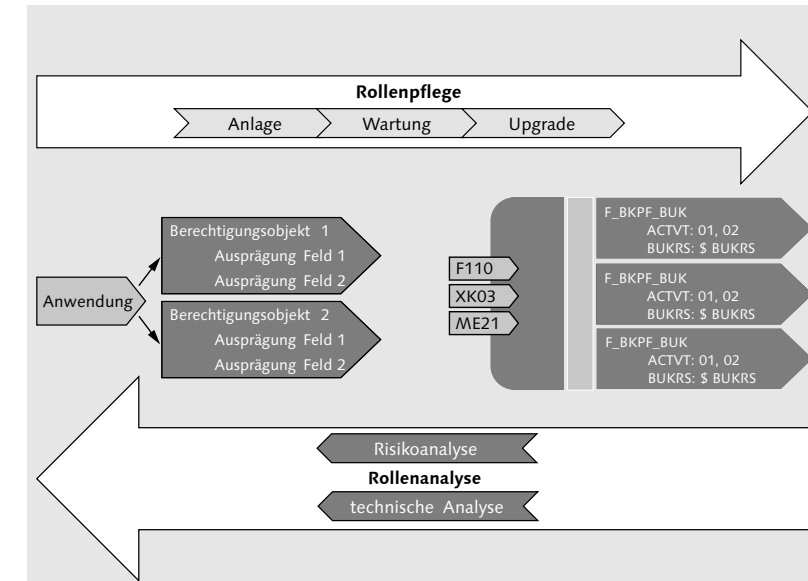


Abbildung 7.1 Berechtigungsvorschlagswerte – Unterstützung bei der Rollenpflege und -analyse

Wir werden im Folgenden darstellen, welchen Nutzen die Vorschlagswertpflege für folgende Bereiche hat:

Nutzen der Vorschlagswerte

- ▶ die Arbeit mit dem Profilgenerator (Anlage und Pflege von Rollen)
- ▶ die Berechtigungspflege beim Upgrade
- ▶ die Nachvollziehbarkeit der Regeleinhaltung
- ▶ ordentlich definierte Risikodefinitionen

In Abschnitt 6.3.1, »Manuelle Profile und Berechtigungen«, sind wir bereits auf die Funktion der Berechtigungsvorschlagswerte für den Profilgenerator eingegangen, die eine umfangreiche Automatisierung der Berechtigungspflege erlauben.

Berechtigungsvorschlagswerte enthalten eine Menge von Berechtigungen in Bezug auf jeweils eine Anwendung. Meistens werden je Anwendung zu mehreren Berechtigungsobjekten notwendige Werte vorgeschlagen. Den überwiegenden Teil dieser Vorschläge liefert

SAP aus. Die Berechtigungsvorschlagswerte müssen organisationspezifisch ergänzt werden. Die Berechtigungsprüfungen sind unabhängig von den Vorschlagswerten, die Prüfung ist Teil des Programms. Die Berechtigungsvorschlagswerte sollten für diese Prüfung möglichst genaue Berechtigungsvorschläge in der Rollenpflege ermöglichen. Bevor wir den Nutzen der Berechtigungsvorschlagswerte darstellen, werden wir Ihnen zunächst ihren Grundzustand und ihre Pflege erläutern.

### 7.1.1 Grundzustand und Pflege der Berechtigungsvorschlagswerte

SAP liefert für alle dazu geeigneten Anwendungen Berechtigungsvorschlagswerte aus. Voraussetzung für die Berechtigungsvorschlagspflege ist, dass diese Berechtigungen im Programmcode der jeweiligen Anwendung als Berechtigungsprüfung implementiert sind. Nur diese Berechtigungsobjekte können als Berechtigungsvorschläge gepflegt werden. Die Berechtigungsprüfung ist allerdings abhängig von der Konfiguration der Prozesse und der Stammdatendefinition. Entschließt sich eine Organisation z. B., optionale Berechtigungsprüfungen einzusetzen, wird dies vermutlich weitere Berechtigungsprüfungen im Programmablauf zur Folge haben. Dieses Prinzip gilt für viele mögliche kundenspezifische Ausprägungen eines Prozesses in den Komponenten. Es gilt aber ebenso für die Integration der Komponenten. Mit anderen Worten: Berechtigungsvorschlagswerte sind teilweise zwingend systemspezifisch. Aus diesem Grund muss die Organisation die Berechtigungsvorschlagswerte entsprechend nachpflegen. Dazu wird die Transaktion SU24 (Pflege der Berechtigungsvorschlagswerte) genutzt.

#### Releasehinweis

Ab dem Basisrelease 7.02 steht eine Reihe neuer Funktionen für die Pflege der Berechtigungsvorschlagswerte zur Verfügung. Die folgenden Ausführungen beziehen sich auf Systeme mit einem Releasestand (SAP\_BASIS) gleich oder größer 7.02.

Abbildung 7.2 verdeutlicht, wie die Pflege von Berechtigungsvorschlagswerten und Berechtigungen in aller Regel erfolgen soll. In der ersten Säule (Entwicklung) sehen Sie die Aufgaben der Entwicklung. Die Entwicklung legt die notwendigen Berechtigungsvorschläge fest.

Die Vorschlagswerte sollten zum Abschluss jeder Entwicklung vollständig vorliegen. Beim »Bauen einer Anwendung« legt die Entwicklung technisch fest, welche Berechtigungsobjekte im Zusammenhang mit einer Anwendung zu prüfen sind: Sie »baut den Authority-Check« mit konkreten Berechtigungsobjekten und ausgewählten Berechtigungswerten. Konkret: Wenn ein Entwickler in eine Anwendung einen Authority-Check z. B. auf M\_BEST\_EKO (Einkaufsorganisation in Bestellung) mit der Aktion ANLEGEN (ACTVT: 01) und die zugehörige Einkaufsorganisation (EKORG: \$EKORG) einbaut, dann weiß er, dass genau diese Berechtigung auch unter der Anwendung geprüft werden wird. Es ist also nur ein sehr geringer Aufwand, an dieser Stelle auch die Berechtigungsvorschlagswerte zu pflegen. Die nachträgliche Ermittlung von Vorschlagswerten beim Testen der Anwendung kostet bereits erheblich mehr. Die »historische« Ermittlung durch Mitarbeiter, die die Anwendung nicht gebaut haben, verursacht nahezu die Kosten eines erneuten Funktions- und Integrationstests.

Um eine nachträgliche Ermittlung der Vorschlagswerte zu umgehen, können Sie den Langzeitberechtigungstrace verwenden (siehe Abschnitt 7.2, »Traces«). Bei diesem Langzeittrace werden schon während der Entwicklung bzw. beim Aufruf der Anwendung Berechtigungsprüfungen getrackt und protokolliert.

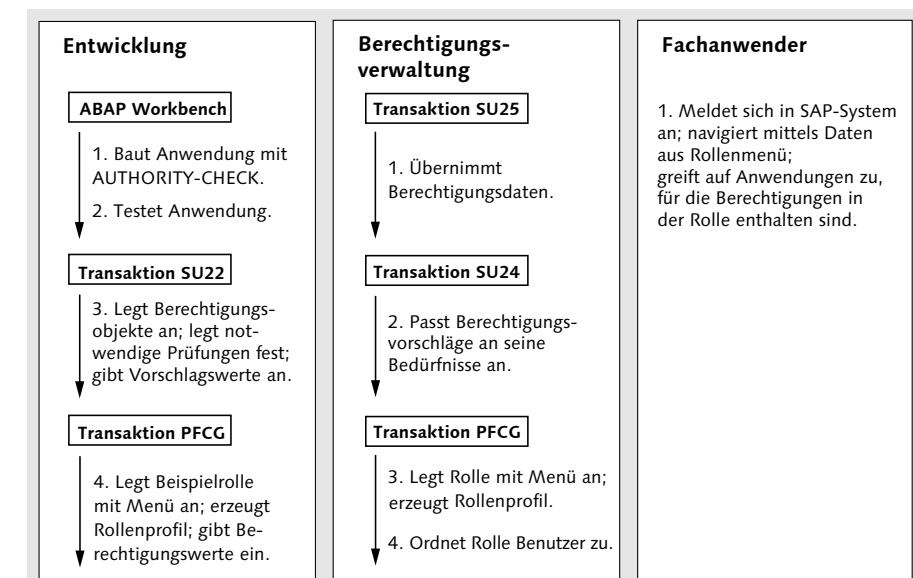


Abbildung 7.2 Von der programmierten Berechtigungsprüfung zur Rolle (nach: <http://help.sap.com>. SAP NetWeaver 7.0 EHP 3)

Für die Pflege von Vorschlagswerten nutzen SAP und ihre Entwicklungspartner die Transaktion SU22 (Berechtigungsvorschlagspflege – SAP). Generell können Sie für die Pflege von Berechtigungsvorschlagswerten die Transaktion SU24 (Berechtigungsvorschlagspflege) nutzen.

Für beide Transaktionen stehen (mittlerweile) Traces als Hilfsmittel zur Verfügung. Dabei handelt es sich um den Berechtigungstrace (siehe Abschnitt 7.2.1, »Vorgehen beim Berechtigungstrace«) und den Systemtrace (siehe Abschnitt 7.2.2, »Vorgehen beim Systemtrace«).

Pflege der  
Vorschlagswert-  
tabelle –  
Kundenwerte

In Abbildung 7.3 ist der Einstiegsbildschirm der Transaktion SU24 (Berechtigungsvorschlagspflege) dargestellt. Die Buttons DOWNLOAD **1** und UPLOAD **2** dienen dem Down- und Upload der Werte; dies kann zur Sicherung oder zur Verteilung zwischen gleich konfigurierten Systemen nützlich sein. Der Button BERECHTIGUNGSVORLAGEN **3** dient der Definition von Berechtigungsvorlagen, die in der Rollenpflege genutzt werden können. Diese Funktion betrachten wir nicht weiter, da wir eine Nutzung nicht empfehlen. Der Button VORSCHLAGSWERTEABGLEICH **4** ermöglicht Ihnen einen selektiven Abgleich von Berechtigungsvorschlagswerten zwischen den SAP-Werten (Transaktion SU22) und den kundeneigenen Werten (Transaktion SU24). Dieser selektive Abgleich ist eine neue Funktion und steht systematisch mit Upgrade-Aktivitäten in Verbindung. Abhängig davon, für welche Anwendung Sie Berechtigungsvorschlagswerte pflegen wollen, selektieren Sie im Selektionsfeld TYP DER ANWENDUNG **5** den entsprechenden Typ. Zur Verfügung stehen die folgenden Anwendungstypen:

- ▶ Transaktion
- ▶ Web-Dynpro-Applikation
- ▶ Web-Dynpro-Anwendungskonfiguration
- ▶ IDoc-Typ
- ▶ Workflowmuster
- ▶ RFC-Funktionsbaustein
- ▶ SAP Gateway: Service Groups Metadata
- ▶ SAP Gateway Business Suite Enablement – Service
- ▶ Zuordnung Service → Berechtigungsobjekt
- ▶ BSP-(Business-Server-Pages-)Applikation


- ▶ JCO-iView
- ▶ People Centric UI Service (CRM)
- ▶ Webservice
- ▶ CRM UIU Component
- ▶ CRM Web Channel Experience Management Module
- ▶ TADIR-Service
- ▶ externer Service
- ▶ Suche nach technischem Namen (Hashcode)



Abbildung 7.3 Einstieg in die Transaktion SU24 (Berechtigungsvorschlagspflege) – Auswahl »Transaktion«

Die Selektion einer Anwendung beeinflusst die weiteren Eingabemöglichkeiten. So sehen Sie die Selektion TRANSAKTIONS-CODE **6**, in die ein oder mehrere Transaktionscodes eingetragen werden können. Unter WEITERE EINSCHRÄNKUNGEN (BERECHTIGUNGS-OBJEKTVERWENDUNG) **7** haben Sie die folgenden Möglichkeiten der Suche:

- ▶ Suche nach Anwendungen für ein bestimmtes Berechtigungsobjekt
- ▶ Suche nach einer Kombination aus Anwendung und Berechtigungsobjekt inklusive Prüfkennzeichen oder Vorschlagsstatus

Die Bearbeitung der Berechtigungsvorschlagswerte wird im Folgebildschirm vorgenommen (siehe Abbildung 7.4). Im mit **1** gekennzeichneten Bereich finden Sie (von links nach rechts) folgende Buttons:

- ▶  (ANZEIGEN < - > ÄNDERN): Mit diesem Button wechseln Sie zwischen Anzeige und Pflege der Berechtigungsvorschlagswerte.

- ▶  (ANDERES OBJEKT): Mit diesem Button können Sie eine andere Anwendung oder ein anderes Objekt auswählen.
- ▶ SAP-DATEN: Hier können Sie sich die SAP-Originaldaten anzeigen lassen.
- ▶ BERECHTIGUNGS-TRACE: EIN oder AUS: Dieser Button informiert Sie zunächst darüber, ob der Berechtigungstrace (siehe Abschnitt 7.2.1, »Vorgehen beim Berechtigungstrace«) eingeschaltet ist. Wenn Sie daraufklicken, erhalten Sie eine Kurzinformation zum Berechtigungstrace.
- ▶ ABMISCHMODUS FÜR PFCG: EIN oder AUS: Über diesen Button erfahren Sie, ob der Abmischmodus für PFCG-Rollen ein- oder ausgeschaltet ist. Werden Änderungen an den Vorschlagswerten vorgenommen, so hat das Einfluss auf die Berechtigungswerte der PFCG-Rollen, die die jeweilige Anwendung im Rollenmenü beinhaltet. Ist der Abmischmodus eingeschaltet, werden betroffene Rollen in den Status PROFILABGLEICH ERFORDERLICH gesetzt und bei der nächsten Änderung der Rolle berücksichtigt. Den Abmischmodus können Sie mittels des Parameters S42X\_SET\_FORCE\_MIX in der Tabelle PRGN\_CUST setzen.
- ▶  Rollen (VERWENDUNG IN EINZELROLLEN): Mithilfe dieses Buttons erhalten Sie Informationen, in welchen PFCG-Einzelrollen die ausgewählte Anwendung im Rollenmenü verwendet wird.

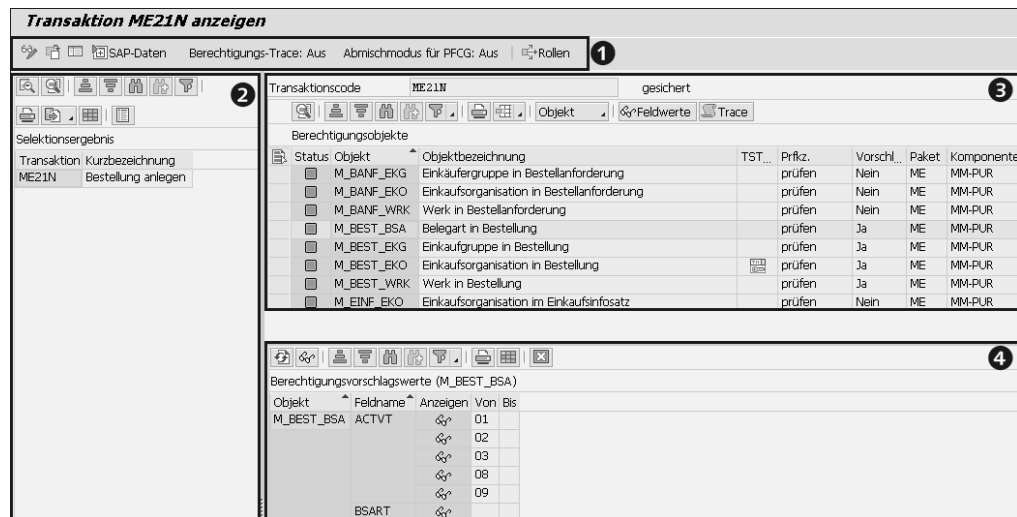










Abbildung 7.4 Transaktion SU24 (Berechtigungs-vorschlagspflege) – Anzeige und Pflege

Im Bereich SELEKTIONSERGEBNIS  sehen Sie die Menge der selektierten Objekte. Dies können, abhängig von der Selektion im Einstiegsbildschirm, entweder Transaktionen, Web-Dynpro-Applikationen, Web-Dynpro-Anwendungskonfigurationen, Workflowmuster, RFC-Funktionsbausteine, TADIR-Services, externe Services etc. sein. Durch Markieren einer Anwendung erscheinen im Bereich BERECHTIGUNGS-OBJEKTE  die jeweils zugehörigen Objekte. Hier pflegen Sie die in Tabelle 7.1 spezifizierten Einstellungen. Dazu müssen Sie zunächst in den Änderungsmodus wechseln. In diesem Bereich sind alle Berechtigungsobjekte enthalten, die im Standard oder in den kundeneigenen Ausprägungen zugeordnet sind. Es handelt sich aber weder um alle Berechtigungsobjekte, die im System zur Verfügung stehen, noch unbedingt um alle, die im Programmablauf tatsächlich geprüft werden.

Im Bereich BERECHTIGUNGSVORSCHLAGSWERTE  können Sie für die in Bereich  ausgewählten Berechtigungsobjekte Vorschlagswerte für die Berechtigungsfelder pflegen.

Im Änderungsmodus werden zusätzliche Buttons angeboten (siehe Abbildung 7.5). Zunächst jedoch sehen Sie im Titel , dass Sie im Änderungsmodus sind. Mit dem Button OBJEKT  können Sie sich (sofern unten ein Objekt selektiert ist) die Objektdefinition, die Objektdokumentation oder den Verwendungsnachweis anzeigen lassen. Sie können aber auch ein Objekt hinzufügen, entweder manuell  oder aus dem Berechtigungstrace  (siehe Abschnitt 7.2.1, »Vorgehen beim Berechtigungstrace«).

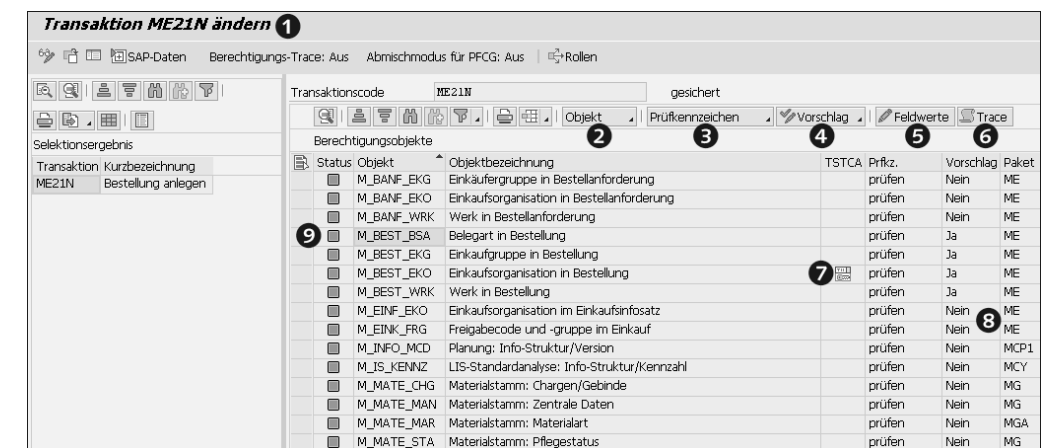


Abbildung 7.5 Transaktion SU24 (Berechtigungs-vorschlagspflege) im Änderungsmodus: Zuordnungen und Status

Mit dem Button PRÜFKENNZEICHEN ③ können Sie festlegen, ob ein Objekt im Programmablauf geprüft werden soll.

Das Prüfkennzeichen kann die in Tabelle 7.1 dargestellten Ausprägungen haben, in der Spalte Funktion wird die Wirkung beschrieben. Auf der folgenden Seite beschreiben wir in einem kurzen Exkurs die Funktion des Kennzeichens »nicht prüfen« etwas genauer.

Funktion	Prfkz.
Prüfkennzeichen wurde nicht spezifiziert – Berechtigungsobjekt wird geprüft.	–
Berechtigungsobjekt wird unter der Anwendung nicht geprüft.	nicht prüfen
Berechtigungsobjekt wird unter der Anwendung geprüft.	prüfen

Tabelle 7.1 Prüfkennzeichen für Berechtigungsobjektprüfungen unter Anwendungen

Sie legen über das Prüfkennzeichen fest, ob ein Objekt unter der Anwendung geprüft werden soll. Das Prüfkennzeichen wird in die Tabelle USOBX\_C (Checktabelle zu Tabelle USOBT\_C) eingetragen und definiert, ob ein Berechtigungsobjekt unter der Anwendung geprüft werden muss. Beachten Sie in jedem Fall, dass Sie die Unterdrückung auch transportieren oder manuell im Zielsystem vornehmen müssen. Da das Unterdrücken der Prüfung kritisch ist, unternehmen wir an dieser Stelle einen Exkurs zum Ausschalten von Prüfungen.

#### Exkurs: Verringerung des Umfangs von Berechtigungsprüfungen

Eine etwaige Unterdrückung der Berechtigungsprüfung kann nur nach genauer Prüfung und Dokumentation der Prüfungsergebnisse vorgenommen werden. Um Prüfungen über die Transaktion SU24 (Berechtigungsobjektprüfungen unter Transaktionen) wirksam unterdrücken zu können, muss der Profilparameter (Parameter `auth/no_check_in_some_cases`) auf Y gesetzt sein (Default). Diese Einstellung ist ebenfalls nötig, um den Profilgenerator überhaupt nutzen zu können.

Berechtigungsprüfungen von Berechtigungsobjekten, die zu Komponenten der Basis oder von SAP ERP Human Capital Management (HCM) gehören, lassen sich nicht unterdrücken.

Bei der Prüfung von Berechtigungskonzepten müssen Sie auf jeden Fall klären, welche Einstellungen zur Unterdrückung von Prüfungen vorge-

nommen wurden. Dabei gilt die Maßgabe, dass SAP-seitig vorgenommene Unterdrückungen Standard sind und kundenseitig angelegte Unterdrückungen erklärungs- und nachweisbedürftig sind.

Die Überprüfung auf Änderungen in diesem Sinne muss als kompensierende Kontrolle durchgeführt werden. Dazu wird die Tabelle USOBX\_C (Checktabelle zu Tabelle USOBT\_C) im Feld OK-KENNZEICHEN mit dem Wert N (keine Berechtigungsprüfung) und dem Feld ÄNDERER = »SAP« ausgewertet.

Über den Button VORSCHLAG ④ in Abbildung 7.5 legen Sie fest, ob und wie das selektierte Berechtigungsobjekt zu einer Anwendung in einer Rolle vorgeschlagen werden soll. Ihre Wahl wird dann in der Spalte VORSCHLAG durch ein JA oder NEIN ⑤ kenntlich gemacht. Die Wirkung ist in Tabelle 7.2 zusammengefasst.

Status	Wirkung
Ja	Das Berechtigungsobjekt wird in einer Rolle vorgeschlagen und muss mit Werten ausgeprägt werden. Einige Felder enthalten bereits Vorschlagswerte.
Ja ohne Werte	Das Berechtigungsobjekt wird in einer Rolle vorgeschlagen. Es gibt allerdings keine gepflegten Vorschläge für Werte.
Nein	Das Berechtigungsobjekt wird nicht vorgeschlagen.
Neu/Ungepflegt	Das Berechtigungsobjekt wird zurückgesetzt und erhält in der Spalte STATUS ⑥ eine rote Ampel.

Tabelle 7.2 Vorschlag und Status

Nachdem Sie das Vorschlagsverhalten festgelegt haben, können Sie nun über den Button FELDWERTE ⑤ detailliert die Werte pflegen, die vorgeschlagen werden sollen. Sinnvollerweise werden nur die Werte eingetragen (Bereich BERECHTIGUNGSVORSCHLAGSWERTE ④ der Abbildung 7.4), für deren Notwendigkeit es einen positiven Nachweis gibt. Dieser Nachweis ist in aller Regel ein Trace. Aus diesem Grund empfehlen wir, über die Auswertung der Traces ⑥ die Berechtigungsvorschlagswerte zu pflegen.

Die Übernahme aus den Traces in die Berechtigungsvorschlagswerte entspricht dem in Abschnitt 6.6, »Vom Trace zur Rolle«, dargestellten Vorgehen. Darum werden wir dies an dieser Stelle nicht weiter ausführen.

Pflege der Berechtigungsvorschlagswerte auf Feldebene

Zur Feldpflege muss das Objekt zum Vorschlag bestimmt sein (Vorschlag JA). Sofern Sie eindeutige Feldwerte ermittelt haben, können diese als Vorschlag eingetragen werden. Sie können keine Organisationsebenen eintragen. Die anderen Werte müssen nach sorgfältiger Prüfung eingetragen werden. Oft besteht die erforderliche Eindeutigkeit nur in Bezug auf die Aktivität.

Sie können das am Beispiel der Bestellung nachvollziehen: Wenn Sie wollen, dass mit der Transaktion ME23N (Bestellung anzeigen) ausschließlich Bestellungen angezeigt werden können, müssten Sie jeweils im Feld ACTVT (AKTIVITÄT) die Werte 03 (ANZEIGEN) und 08 (ÄNDERUNGSBELEGE ANZEIGEN) mitgeben. Da es aber wahrscheinlich erforderlich ist, den Zugriff organisatorisch zu differenzieren, können Sie im Feld BELEGART IN BESTELLUNG (BSART) keinen Wert eintragen, da die Belegart ein ablauforganisatorisches Kriterium ist und Sie den Zugriff wahrscheinlich für einzelne Belegarten unterschiedlich ausprägen wollen.

Dieses Vorgehen ist erforderlich, um einerseits das Berechtigungsobjekt und die Aktivität automatisch vorgeschlagen zu bekommen. Andererseits wollen Sie verhindern, dass Sie das Feld BELEGART ändern müssen, da dies den Status des Objekts auf VERÄNDERT im Profil setzen würde.

#### Enjoy-Transaktionen

Die Transaktionen zur Bestellung sind deswegen ein gutes Beispiel, weil sie als Enjoy-Transaktionen prinzipiell vergleichbare Aktionen erlauben: Wenn die entsprechenden Berechtigungen zur Transaktion vergeben sind, kann aus der Transaktion ME23N (Bestellung anzeigen) eine Bestellung auch angelegt oder geändert werden (siehe SAP-Hinweis 751129 – Berechtigungen in Enjoy-Transaktionen im Einkauf). Die zu pflegenden Werte ergeben sich aus Ihrer Nutzung der Enjoy-Logik. Für das Beispiel der Transaktion ME23N (Bestellung anzeigen) heißt das:

- ▶ ausnahmslos Enjoy-Logik nutzen = Anlegen, Ändern, Anzeigen
- ▶ überwiegend Enjoy-Logik nutzen = keine Werte
- ▶ Enjoy-Logik nicht nutzen = Anzeigen

Berechtigungs vorgeschlagswerte stellen die mächtigste positiv regelbasierte Steuerung von Berechtigungen dar. Sie verleiten allerdings unter Umständen dazu, sie einfach zu übernehmen. Das kann jedoch falsch sein: Wenn Sie also die Transaktion ME23N (Bestellung anzeigen) tatsächlich nur zum Anzeigen nutzen wollen, wenn Sie aber die

Werte ANLEGEN, ÄNDERN und ANZEIGEN zulassen, wird mit Sicherheit irgendwann dieser Wert auch so in eine Rolle, die nur das Anzeigen erlauben soll, aufgenommen.

#### Obligatorischer Transportauftrag

Sämtliche Änderungen der Berechtigungsvorschlagswerte werden in einen Transportauftrag übernommen. Dabei sollten Sie die üblichen Empfehlungen zur Transport Policy und Ihre hauseigene Policy beachten.

Änderungen der Vorschläge für den Profilogenerator werden in unterschiedliche Tabellen geschrieben. Die Tabelle USOBT (Relation Transaktion R Ber.objekt) enthält die Auslieferungsdaten für Vorschläge. Die kundenseitigen Änderungen der Berechtigungsvorschlagswerte werden in die Tabelle USOBT\_C (Relation Transaktion R Berechtigungsobjekt – Kunde) eingetragen. Die Tabelle USOBX (Checktabelle zu Tabelle USOBT) enthält die Auslieferungsdaten für Prüfkennzeichen. Die kundenseitigen Änderungen der Prüfkennzeichen werden in die Tabelle USOBX\_C (Checktabelle zu Tabelle USOBT\_C) eingetragen.

In Abbildung 7.6 sind beispielhaft drei Änderungen vorgenommen: In Bezug auf die Transaktion ME21N (Bestellung anlegen) wurde das Berechtigungsobjekt F\_FICA\_FOG (Haushaltsmanagement: Berechtigungsgruppe des Fonds) auf »nicht prüfen« gesetzt ❶, das Berechtigungsobjekt F\_FICA\_FCD – (Haushaltsmanagement Fonds) wurde auf Vorschlag JA gesetzt ❷, und im Feld AKTIVITÄT BERECHTIGUNGSPRÜFUNG (FM\_AUTHACT) ❸ wurden die Aktionen 01, 02, 08 und 10 eingetragen.

Vorschlagswert-  
tabellen und  
ihre Relation

Status	Objekt	Objektbezeichnung	TSTCA	Prfz.	Vorschlag	Paket
	F_BKPF_KOA	Buchhaltungsbeleg: Berechtigung für Kontoarten		prüfen	Nein	FBAS
	F_FICA_CTR	Haushaltsmanagement: Finanzstelle		prüfen	Nein	FMBS
	F_FICA_FCD	Haushaltsmanagement: Fonds		prüfen	Ja	FMBS
	F_FICA_FOG	Haushaltsmanagement: Berechtigungsgruppe des Fonds		❶ nicht prüfen	Nein	FMBS
	F_FICA_FPG	Haushaltsmanagement: Berechtigungsgruppe der Finanzpostion		prüfen	Nein	FMBS
	F_FICA_FSG	Haushaltsmanagement: Berechtigungsgruppe der Finanzstelle		prüfen	Nein	FMBS
	F_FICA_FTR	Haushaltsmanagement: Finanzbudgetkonto		prüfen	Nein	FMBS
	F_FICA_TRG	Haushaltsmanagement: Berechtigungsgruppen der H+M-Kontierung		prüfen	Nein	FMBS

Objekt	Feldname	Ändern	Von	Bis
F_FICA_FCD	FM_AUTHACT		01	10
			02	
			08	
			10	
FM_FIKRS				\$FIKRS
FM_FINCODE				

Abbildung 7.6 Exemplarische Pflege von Berechtigungsobjekten



Diese Änderungen wirken sich nicht auf die Tabelle USOBT (Relation Transaktion → Ber.objekt) und die Tabelle USOBX (Checktabelle zu Tabelle USOBT) aus. Stattdessen werden die Werte in die Tabelle USOBT\_C (Relation Transaktion → Berechtigungsobjekt – Kunde) und die Tabelle USOBX\_C (Checktabelle zu Tabelle USOBT\_C) eingetragen.

In der Tabelle USOBT\_C (Relation Transaktion R Berechtigungsobjekt – Kunde) ergeben sich durch die Änderung die in Tabelle 7.3 dargestellten Einträge. Aus der Tabelle sind zur Vereinfachung nur die folgenden Spalten dargestellt:

- ▶ Object = Berechtigungsobjekt
- ▶ Field = Berechtigungsfield
- ▶ Low = Einzelwert oder der kleinste Wert eines Intervalls
- ▶ Modifier = letzter Änderer
- ▶ Modified = Kennzeichen für Änderung

OBJECT	FIELD	LOW	MODIFIER	MODIFIED
F_FICA_FCD	FM_AUTHACT	01	I055366	X
F_FICA_FCD	FM_AUTHACT	02	I055366	X
F_FICA_FCD	FM_AUTHACT	08	I055366	X
F_FICA_FCD	FM_AUTHACT	10	I055366	X
F_FICA_FCD	FM_FIKRS	\$FIKRS	I055366	X
F_FICA_FCD	FM_FINCODE		I055366	X

Tabelle 7.3 Tabelle »Relation Transaktion ? Ber.objekt (Kunde)« nach Anpassung

Die erste Zeile bedeutet also, dass im Berechtigungsobjekt F\_FICA\_FCD das Feld FM\_AUTHACT mit dem generischen Wert \* durch den Benutzer I055366 geändert wurde.

In der Tabelle USOBX\_C (Checktabelle zu Tabelle USOBT\_C) ergeben sich die in Tabelle 7.4 dargestellten Einträge.

OBJECT	MODIFIER	OKFLAG	MODIFIED
F_FICA_FCD	I055366	Y	X
F_FICA_FOG	I055366	N	X

Tabelle 7.4 Tabelle »Checktabelle zu Tabelle USOBT\_C« nach Anpassung

Die Änderungshistorie können Sie den in Tabelle 7.5 benannten Tabellen entnehmen.

Tabelle	Bezeichnung
USOBT_CD	Änderungshistorie für Feldwerte
USOBX_CD	Änderungshistorie zu Prüfkennzeichen

Tabelle 7.5 Weitere Tabellen zu Berechtigungsvorschlagswerten

Wenn die Berechtigungsvorschlagswerte gut gepflegt und in den Rollen entsprechend verwendet werden, kann ein Upgrade zügig durchgeführt werden. Zum Upgrade kommen wir im nächsten Abschnitt.

Der Vollständigkeit halber kommen wir noch einmal auf Abbildung 7.5 zurück. Dort hatten wir noch nicht darauf hingewiesen, dass ein Startberechtigungsobjekt in der Spalte TSTCA dieser Abbildung unter ⑦ besonders gekennzeichnet ist.

### 7.1.2 Nutzen der Berechtigungsvorschlagswerte

Eine umfassende Pflege der Berechtigungsvorschlagswerte in Verbindung mit dem angegebenen Statusziel hat folgenden Nutzen:

#### ▶ Funktion für den Profilgenerator

Berechtigungspflege erfolgt regelbasiert statt *by incident*. Konkret wird eine technische Regel hinterlegt, welche Berechtigungsobjekte mit welchen Feldwerten zu einer Anwendung (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) gehören und somit in den Berechtigungen einer Rolle vorgeschlagen werden sollen. Da diese Feldwerte, Aktivitäten und differenzierenden Merkmale die konkrete Nutzung bestimmen, ist diese technische Regel auch gleichzeitig eine Norm in Bezug auf die statthaften Aktivitäten (z. B. Vorerfassen) einer Verrichtung (z. B. Belegbearbeitung). Diese Normbildung unterstützt die Regelkonformität und die Transparenz über die Erreichung der Regelkonformität. Eine detaillierte Beschreibung dazu finden Sie im Unterabschnitt »Funktion für den Profilgenerator« in diesem Abschnitt.

Eine weitere Funktion für den Profilgenerators ist es, Erfahrungswissen zu sichern, indem Sie nicht jedes Mal neu ermitteln müssen, welche Berechtigungsobjekte für eine bestimmte Anwendung

(Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) nötig sind. Diese Funktion steigert die Effizienz und Nachhaltigkeit.

Schließlich ermöglicht die Pflege über den Profilvergenerator, Rollen sauber zu halten (entzogene Anwendungen – Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc. – führen zum Entzug von Berechtigungen), auch diese Funktion sichert Regelkonformität.

#### ► Funktion im Upgrade

Die Pflege der Berechtigungsvorschlagswerte soll die Upgrade-Kosten angemessen halten. Diese Funktion ist Ausdruck der Effizienz, die bei präziser Pflege erreicht werden kann. Mehr dazu erfahren Sie im Unterabschnitt »Funktion im Upgrade« in diesem Abschnitt.

#### ► Normativer Nutzen

Pflege der Berechtigungsvorschlagswerte soll die Auditierbarkeit sicherstellen. Der technisch definierte Zusammenhang zwischen Anwendung (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) und Berechtigungsobjekt erleichtert sinnvolle Audits von Berechtigungskonzepten. Ausführliche Informationen dazu finden Sie im Unterabschnitt »Normativer Nutzen« in diesem Abschnitt.

#### ► Nutzen für die Risikoanalyse

Die Pflege der Berechtigungsvorschlagswerte soll sicherstellen, dass bei der Definition von Risiken in einem Werkzeug wie SAP Access Control die »richtigen« Werte genutzt werden. Alle selbst erstellten Risikodefinitionen basieren auf den Werten der Vorschlagstabellen. Dazu finden Sie eine detaillierte Beschreibung im Unterabschnitt »Nutzen der Berechtigungsvorschlagswerte für Risikoanalyse und externe Rollenpflegetools« in diesem Abschnitt.

Die Pflege der Berechtigungsvorschlagswerte für den Profilvergenerator vereinfacht mittelfristig die Rollenpflege und macht sie transparenter.

#### Funktion für den Profilvergenerator

Die Berechtigungsvorschlagswerte für Berechtigungen werden – im Kundensystem – über die Transaktion SU24 (Pflege der Zuordnungen von Berechtigungsobjekten zu Transaktionen) gepflegt. Sie ver-

sorgen den Profilvergenerator mit Vorschlägen für Berechtigungswerte. Jede im Menü eingefügte Anwendung (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) wird mit diesen Default-Werten versorgt. Abbildung 7.7 verdeutlicht, dass in Bezug auf die im Menü vergebene Anwendung die Berechtigungsvorschlagswerte in die Berechtigungen zur Rolle übernommen werden.

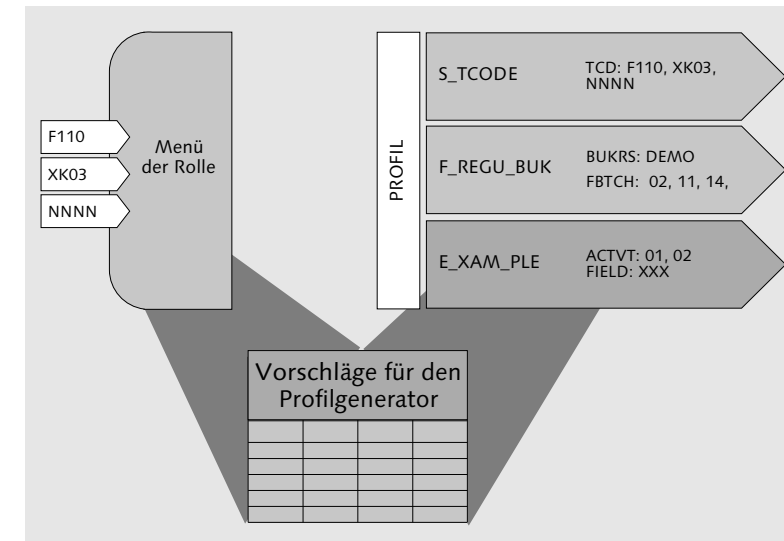


Abbildung 7.7 Übernahme der Berechtigungsvorschlagswerte für die im Menü vergebenen Anwendungen (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.)

Die Übernahme von Berechtigungsvorschlagswerten funktioniert bei der Rollenänderung im Menü entweder, indem Sie auf der Registerkarte BERECHTIGUNGEN den Button BERECHTIGUNGSDATEN ÄNDERN wählen oder auf den Button EXPERTENMODUS ZUR PROFILGENERIERUNG klicken und dort ALTEN STAND LESEN UND MIT DEN NEUEN DATEN ABGLEICHEN auswählen. Die Pflege über den Expertenmodus sollte der Standard sein, da Sie in diesem Fall selbst festlegen, wie sich der Profilvergenerator verhalten soll. Nach der Selektion springen Sie in die Pflege der Berechtigungen. Dabei fallen die unterschiedlichen Status der Berechtigungen auf, die wir schon in Abschnitt 6.3.2, »Rollenpflege«, erläutert haben.

Berechtigungsobjekte können vier Status haben:

- MANUELL: Das ganze Objekt wurde manuell hinzugefügt.
- VERÄNDERT: Der Vorschlagswert wurde verändert.

Übernahme von Berechtigungsvorschlagswerten

- ▶ **GEPFLEGT:** Entspricht dem Vorschlagswert, es wurden offene Felder gepflegt.
- ▶ **STANDARD:** Entspricht dem Vorschlagswert.

Der Unterschied zwischen Pflegen und Verändern besteht darin, dass bei der Pflege offene Felder gepflegt, bei der Veränderung dagegen Standardfeldausprägungen verändert werden.

Status und Entzug von Anwendungen

Dieser Unterschied ist relevant. Der Mechanismus, der beim Ergänzen einer Rolle um eine Anwendung (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) abläuft, arbeitet analog beim Entziehen einer Anwendung. Die Berechtigungsobjekte im Status **GEPFLEGT** oder **STANDARD**, die ausschließlich zur entzogenen Anwendung gehören, werden wieder entzogen. Damit wird einem Kernproblem oft veränderter Rollen vorgebeugt: dem Problem, dass es keine nachhaltige logische Zuordnung von enthaltenen Berechtigungsobjekten zu den vergebenen Anwendungen gibt.

#### Beispiel: Verwendung von Berechtigungsobjekten in Rollen und deren Pflegestatus

Dies soll an einem Beispiel dargestellt werden: Einer Rolle, die ausschließlich Reporting-Transaktionen enthält, wird die Transaktion SQVI (QuickViewer) hinzugefügt. Da das Berechtigungsobjekt für Tabellenzugriffe (S\_TABU\_DIS) kein Standardvorschlag ist, wird es manuell der Rolle hinzugefügt. Später wird – ganz im Sinne wünschenswerter Regelkonformität – die Nutzung des QuickViewers massiv eingeschränkt, die Transaktion wird der Reporting-Rolle entzogen. Da das Berechtigungsobjekt für Tabellenzugriffe manuell hinzugefügt wurde, verbleibt es in der Rolle. Das hat Folgen:

- ▶ Die Rolle enthält mehr Berechtigungen als erforderlich.
- ▶ Das Risiko, das in einer Kombination mit anderen Rollen entstehen kann, ist erheblich und nicht vorab zu bestimmen.

Je präziser die Default-Werte in den Tabellen gepflegt sind, desto genauer passen die Berechtigungsvorschlagswerte für die Rollen. Anzustreben ist minimal ein Zustand, in dem auf Objektebene 95 % aller Berechtigungsobjekte als Default in die Rolle übernommen werden. Das heißt, dass nur noch 5 % der Berechtigungsobjekte mit dem Status **VERÄNDERT** gekennzeichnet sind.

Da Berechtigungsausprägungen immer einen kundenspezifischen Anteil haben, d. h. durch die Konfiguration, das Stammdatenkon-

zept, aber auch individuelle Präferenzen bestimmt werden, sind die Standardberechtigungsvorschlagswerte unvollständig.

#### Standardvorschläge pflegen

Wir empfehlen Ihnen die detaillierte Pflege der Berechtigungsvorschlagswerte ausdrücklich auch für Standardanwendungen (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.), da sinnvolle Berechtigungsvorschlagswerte gegebenenfalls besondere Nutzungen, Systemeinstellungen und Stammdatenmerkmale reflektieren.

#### Funktion im Upgrade

Mit der Transaktion SU25 (Upgrade-Tool für den Profilogenerator) werden verschiedene Schritte vollzogen, um im Upgrade die alten Berechtigungen und Rollen den neuen Erfordernissen anpassen zu können. Im Prinzip werden dort die alten Berechtigungsvorschlagswerte (Kunde) mit den neuen Berechtigungsvorschlagswerten (SAP) abgemischt und die Rollen mit Änderungsbedarf identifiziert. Die Upgrade-Nacharbeiten bezüglich Berechtigungen selbst werden in Abschnitt 7.3, »Upgrade-Nacharbeiten von Berechtigungen«, beschrieben.

#### Normativer Nutzen

Aus den in Kapitel 4, »Rechtlicher Rahmen – normativer Rahmen«, angeführten Gründen sind immer nur die nachweislich notwendigen Berechtigungen zu vergeben. Soll ein Mitarbeiter Bestellungen ändern dürfen, dann muss er einen Benutzer im System mit genau diesen Berechtigungen bekommen. Technisch sollte dabei ein Zustand erreicht werden, in dem durch das Einfügen der Transaktion ME21N (Bestellung anlegen) alle notwendigen Berechtigungsobjekte mit allen erforderlichen aktivitätsbezogenen Feldwerten vorgeschlagen werden. Auf diese Weise müssen anschließend nur noch die organisatorischen Werte wie Werk/Belegart u. Ä. eintragen werden. Wird so vorgegangen, kann auch der Auditor nachvollziehen, dass die Ausprägung der Berechtigungen den im System hinterlegten Regeln entspricht. Stellen Sie sich eine Rolle mit 100 Anwendungen, 40 Berechtigungsobjekten und 120 Feldausprägungen in den Berechtigungsobjekten vor. Wenn sämtliche Objekte manuell hinzugefügt wurden, können Sie nicht mehr erkennen, welche Berechtigungsobjektausprägung für eine bestimmte Anwendung erforderlich ist und

ob für die 100 Anwendungen wirklich nur notwendige Werte vergeben wurden. Während Sie für eine Anwendung dies gegebenenfalls über einen Trace beweisen können, dürfte der Aufwand für 100 Anwendungen meistens zu groß sein.

Wenn Berechtigungsobjekte manuell einem Profil hinzugefügt oder geändert wurden, besteht keine Relation zwischen dem Umfang an Anwendungen der Rolle (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) und den zugeordneten Berechtigungsobjekten. Das bedeutet, dass keine Auskunft darüber möglich ist, warum etwa ein kritisches Objekt einer Rolle zugeordnet wurde.

Vorschlagstabelle  
und Regel-  
konformität

Es besteht ein direkter Zusammenhang zwischen der Nutzung der Berechtigungsvorschlagswerte und der Regelkonformität von Berechtigungen. Berechtigungen können in einem komplexen System wie SAP ERP nur dann regelkonform sein, wenn sie technischen Regeln folgen – das sind die Berechtigungsvorschlagswerte.

#### Ohne Nachvollziehbarkeit keine wirksame Prüfung

Nur wenn nachvollziehbar bleibt, warum welche Berechtigungsobjekte und Werte vergeben wurden, kann die Regelkonformität von Rollen effizient geprüft werden. Diese Prüfbarkeit entsteht über die Berechtigungsvorschlagswerte.

Im Sinne eines umfassenden Verständnisses des Internen Kontrollsystems (IKS) ist ein Nachweis erforderlich, warum welcher Benutzer welche Berechtigungen hat, also auch warum eine Rolle ein bestimmtes Berechtigungsobjekt enthält. Dieser Nachweis auf Objektebene ist ohne vorschlagswertbasierte Pflege nicht möglich. Die Vorschlagswertpflege ist in diesem Sinne eine Normsetzung, wie Berechtigungen angesteuert werden dürfen. Die Umsetzung ist der Nachweis, ob die Norm eingehalten wurde. Die Norm selbst ist Ausdruck eines technisch detaillierten IKS.

#### Nutzen der Berechtigungsvorschlagswerte für Risikoanalyse und externe Rollenpfegetools

Eine detaillierte Analyse von Funktionstrennungskonflikten und kritischen Transaktionen kann nur durchgeführt werden, wenn die kundenspezifischen Berechtigungsvorschlagswerte eingeschlossen werden: Die Präzisierung der Berechtigungsvorschlagswerte stellt eine Präzisierung der notwendigen Werte für Zugriffe und somit für Risiken dar. Diese Systematik ist u. a. in der Definition neuer Risiken in SAP Access Control enthalten.

Um das an einem Beispiel darzustellen: Das mit dem Anlegen einer Bestellung verbundene Risiko wird dargestellt, indem zunächst festgestellt wird, dass die Transaktion ME21N notwendig ist. Diese sehr einfache Risikodefinition ist in Tabelle 7.6 zusammengefasst.

Anwendung	Berechtigungsobjekt	Feld	Ausprägung
ME21N	S_TCODE	TCD	ME21N

Tabelle 7.6 Einfache Risikodefinition

Mit dieser Transaktion allein kann ein Benutzer nicht viel anfangen, er benötigt in jedem Fall noch drei Berechtigungsobjekte mit den entsprechenden Ausprägungen. Mit anderen Worten: Die in Tabelle 7.6 dargestellte Definition ist zu einfach, sie wird zu falschen Befunden führen, denn jeder, der die Transaktion ME21N (Bestellung anlegen) überhaupt hat, wird erfasst.

Dementsprechend muss die Risikodefinition ergänzt werden, um sicherzustellen, dass auch nur die echten Risiken nachgewiesen werden. Dies ist exemplarisch in Tabelle 7.7 dargestellt. Wie detailliert ein Risiko zu beschreiben ist, behandeln wir in Kapitel 11, »SAP Access Control«. An dieser Stelle soll nur Folgendes deutlich werden: Ohne die Berechtigungsvorschlagswerte können Sie ein Risiko nur präzise definieren, indem Sie ersatzweise Transaktion für Transaktion tracen.

Gute Berechtigungs-  
vorschlags-  
werte – präzise  
Risikodefinitionen

Anwendung	Berechtigungsobjekt	Feld	Ausprägung
ME21N	S_TCODE	TCD	ME21N
		ACTVT	01
	M_BEST_BSA	BSART	FO, NB
		ACTVT	01
	M_BEST_EKG	EKGRP	\$EKGRP
		ACTVT	01
	M_BEST_EKO	EKORG	\$EKORG
		ACTVT	01

Tabelle 7.7 Präzise Risikodefinition

Das Gleiche gilt sinngemäß für alle Risikoanalyselösungen – inklusive der selbst gebauten. Sind diese nicht mit den Vorschlagstabellen integriert, können sie nicht dauerhaft die Rollenpflege Upgrade-

sicher und regelkonform vereinfachen. Das gilt auch für die Nutzung des Business Role Managements von SAP Access Control. Die Nutzung im Rollenmanagement und in der Risikoanalyse wird in Abbildung 7.8 verdeutlicht. Zu sehen ist, dass die Werte der Tabelle USOBT\_C einerseits in der Risikoanalyse und andererseits im Rollenmanagement Verwendung finden.

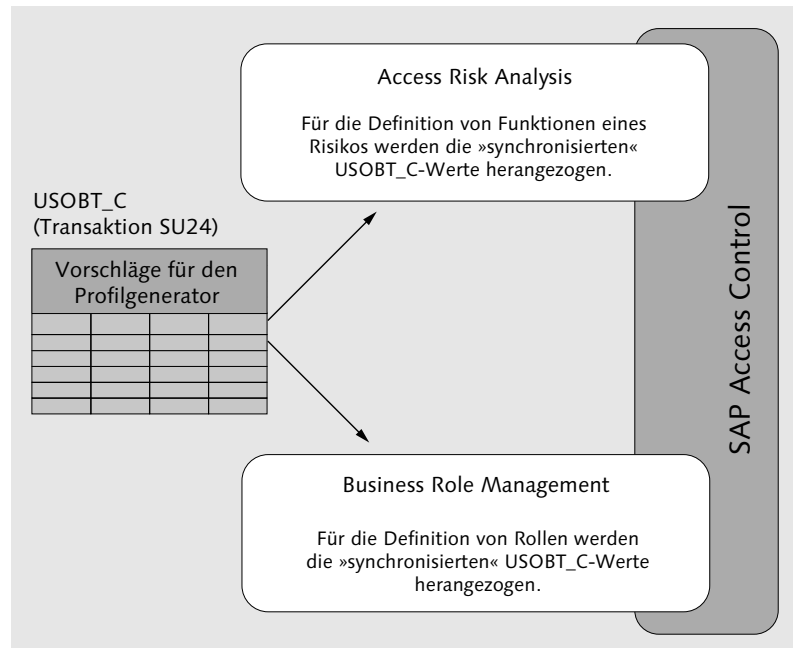


Abbildung 7.8 Nutzung der Berechtigungsvorschlagswerte für die Risikoanalyse und externe Rollenpfegelösungen

## 7.2 Traces

In Abschnitt 7.1.1, »Grundzustand und Pflege der Berechtigungsvorschlagswerte«, wurde der Trace als Hilfsmittel für die Ermittlung der relevanten Vorschlagswerte und in Abschnitt 6.6, »Vom Trace zur Rolle«, als Hilfsmittel für die Rollenpflege und für die Vorschlagswertpflege dargestellt. In diesem Abschnitt sollen die beiden Traces systematisch erläutert werden. Ein Trace ist in unserem Kontext und stark vereinfacht eine Aufzeichnung von Benutzeraktionen und Systemreaktionen.

### Hinweis aus der Entwicklung

Ein Entwickler braucht für seine Anwendung keinen Trace, er kann aus den von ihm »eingebauten« Berechtigungsprüfungen unmittelbar die notwendigen Berechtigungsvorschläge ohne nennenswerten Aufwand festlegen.

Es stehen Ihnen drei Arten von Traces zur Verfügung: der Berechtigungstrace, der Systemtrace und der Benutzertrace:

Tracearten

Für die erste Befüllung der Tabelle USOBT\_X (Checktabelle zu Tabelle USOBT) für den Profilgenerator wird SAP-intern der Berechtigungstrace genutzt. Dieser wird meistens als Langzeittrace verwendet, der mandantenübergreifend und benutzerunabhängig Daten sammelt und in der Datenbank ablegt. Sobald der Trace während der Ausführung eines Programms auf eine Berechtigungsprüfung stößt, die im Zusammenhang mit der aktuellen Anwendung bislang nicht erfasst war, legt er einen entsprechenden Eintrag in der Tracedatenbanktabelle an. Das bedeutet, dass Sie die Anwendung möglichst vollständig testen müssen, um aussagekräftige Tracedaten zu erhalten. Um den Trace auswerten zu können, müssen Sie ihn vor dem Testen/Aufzeichnen aktivieren und die wesentlichen Aktionen lokal oder im Zielsystem ausführen.

Berechtigungstrace

In SAP-Hinweis 543164 (Bedeutung der Werte von `auth/authorization_trace`) wird deutlich darauf hingewiesen, dass dieser Trace die Performance verringert und vom Kunden auf eigenes Risiko eingesetzt wird. Sinnvoll ist dieser Trace, um die Berechtigungsprüfungen von kundeneigenen Programmen in die Berechtigungsvorschlagswerte zu übertragen. Diese Übertragung ist eine manuelle Übernahme, da eine Bewertung erfolgen muss. Es ist ab Basisrelease 7.02 nicht mehr erforderlich, dazu die Transaktion SU22 (Berechtigungsvorschlagspflege – SAP) zu verwenden. Wie schon ausgeführt, steht für die Pflege von Berechtigungsvorschlagswerten die Transaktion SU24 (Berechtigungsvorschlagspflege) zur Verfügung. Dort können auch die Werte des Berechtigungstrace angezeigt werden, wie wir im Folgenden erläutern werden. Wir raten Ihnen dringend, diesen Profilparameter in produktiven Systemen inaktiv zu setzen – dies ist auch Auslieferungsstandard. Es ist aber durchaus empfehlenswert, diesen Trace auf dem Entwicklungs- und gegebenenfalls auch auf dem Qualitätssicherungssystem zu aktivieren, so sammeln Sie bereits während der Entwicklung von neuen Funktionen die ent-

sprechenden Berechtigungsvorschlagswerte. Profilparameter können über die Transaktion RZ11 (Pflege der Profilparameter) geändert werden.

**Systemtrace** Der Systemtrace (Transaktion ST01 oder STAUTHTRACE) ist ein Kurzzeittrace, der mandantenabhängig und nur auf dem aktuellen Anwendungsserver Berechtigungsdaten sammelt. In die Rollenpflege und die Vorschlagswertpflege müssen über RFC auch die Traceergebnisse aus beliebigen Zielmandanten eingebunden werden. Auch dieser Trace kann über RFC auf beliebigen Mandanten ausgeführt sowie ausgewertet werden.

**Benutzertrace** Der Benutzertrace ist ein neuer Trace, der ab SAP NetWeaver 7.40 verfügbar ist (siehe SAP-Hinweis 2220030). Er ist ebenfalls als Langzeittrace konzipiert, sammelt aber im Gegensatz zum Berechtigungstrace mandanten- und benutzerabhängige Berechtigungsdaten. Diese werden wie beim Berechtigungstrace in der Datenbank abgelegt. Analog zum Berechtigungstrace erfolgt die Aufzeichnung der Berechtigungsprüfungen. Dabei werden die laufende Anwendung mit der Programmstelle, das Berechtigungsobjekt und dessen geprüfte Werte sowie das Ergebnis der Berechtigungsprüfung pro Benutzer einmal gespeichert. Sie haben die Möglichkeit, die Aufzeichnung auf den Anwendungstyp, die Benutzer und die Berechtigungsobjekte hin zu filtern. Für den Filter können Sie zwei unterschiedliche Anwendungstypen, bis zu zehn Benutzer und bis zu zehn Berechtigungsobjekte festlegen.

Der Benutzertrace wird über den Profilparameter `auth/auth_user_trace` aktiviert. Sollten Sie den Benutzertrace mit einem Filter aktiviert haben, müssen Sie in der Transaktion STUSERTRACE auch einen Filter definieren, denn sonst wird nichts aufgezeichnet. Auch für den Benutzertrace gilt, dass die Aktivierung ohne einen Filter zu hohen Performanceeinbußen führen kann. Prüfen Sie daher die möglichen Anwendungsszenarien immer auch im Hinblick auf die Auswirkungen auf die Performance. Der Benutzertrace ist hilfreich bei Szenarien, in denen Sie spezielle Benutzer oder Berechtigungsobjekte auswerten wollen. Sie können z. B. die erforderlichen Berechtigungen für Batch-Benutzer oder Tabellenzugriffe über `S_TABU_NAM` aufzeichnen.

### 7.2.1 Vorgehen beim Berechtigungstrace

Zunächst müssen Sie die Transaktion RZ11 (Pflege der Profilparameter) aufrufen und den Parameter `auth/authorization_trace` eingeben (siehe Abbildung 7.9).

Abbildung 7.9 Profilparameterpflege für Berechtigungstrace

Klicken Sie auf den Button ANZEIGEN. Auf dem nächsten Bild PROFILPARAMETEREIGENSCHAFTEN klicken Sie auf den Button WERT ÄNDERN (siehe Abbildung 7.10).

Metadaten für Parameter auth/authorization_trace	
Beschreibung	Wert
Name	auth/authorization_trace
Typ	Zeichenfolge
Weitere Auswahlkriterien	{Y y N n F f  }{0,1}
Einheit	
Parametergruppe	Auth
Parameterbeschreibung	Trace every authority-check once for authorization proposals
CSN-Komponente	BC-SEC-AUT-PFC
Systemweiter Parameter	Nein
Dynamischer Parameter	Ja
Vektorparameter	Nein
Enthält Subparameter	Nein
Prüffunktion existiert	Nein

Werte des Profilparameters auth/authorization_trace	
Auflösungsstufe	Wert
Kernel-Default	
Default-Profil	
Instanz-Profil	
Aktueller Wert	

Abbildung 7.10 Profilparametereigenschaften

Auf dem folgenden Bild setzen Sie den Wert auf Y (aktiv) oder F (aktiv mit Filter) (siehe Abbildung 7.11). Den Filter für diesen Trace

können Sie über die Transaktion STUSOBTRACE festlegen und anhand der Kriterien Typ der Anwendung, Berechtigungsobjekte oder Benutzer einschränken. Den Warnhinweis **ÄNDERUNG NICHT PERMANENT, GEHT NACH DEM NEUSTART DES SERVERS VERLOREN** bestätigen Sie, und anschließend bestätigen Sie Ihre Eingabe. Der Trace ist nun aktiv.

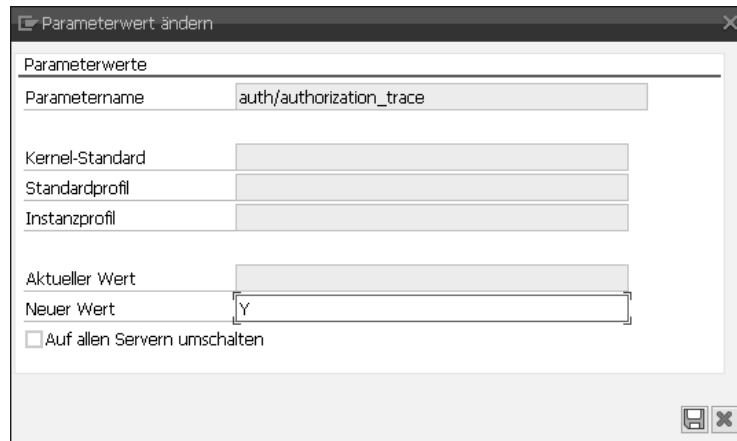


Abbildung 7.11 Parameterwert setzen

**Transaktionen tracen**

Führen Sie nun die Anwendung(en) aus, für die Sie die notwendigen Berechtigungsobjekte ermitteln wollen. In unserem Beispiel ist es die Transaktion, die wir in Abschnitt 7.7.1 angelegt haben, also eine Parametertransaktion zur Pflege von Tabellen über definierte Views.

Die Ergebnisse dieses Trace werden in die Tabelle USOB\_AUTHVALTRC geschrieben und können ebenfalls in der Transaktion STUSOBTRACE über einen Klick auf den Button AUSWERTEN eingesehen werden (siehe Abbildung 7.12).

**Eintrag in die Berechtigungs-vorschlagspflege**

Für die Auswertung ist die Einschränkung TYP DER ANWENDUNG: TRANSAKTION ausgewählt worden, damit nur Tracedaten für neue Transaktionen angezeigt werden. Die Auswertung (siehe Abbildung 7.13) listet nun für jede Transaktion Berechtigungsobjekte mit den geprüften Berechtigungswerten auf. Diese Informationen können Sie als Grundlage zur Pflege von Berechtigungsvorschlagswerten oder in der Rollenpflege verwenden.

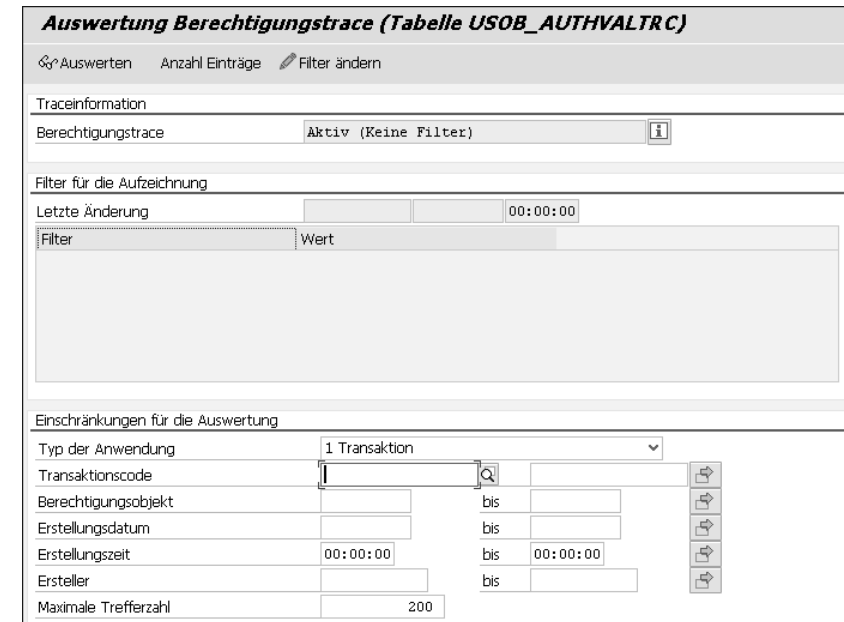


Abbildung 7.12 Auswertung des Berechtigungstrace über Transaktion STUSOBTRACE

**Berechtigungstrace (Tabelle USOB\_AUTHVALTRC): 25 Treffer**

Typ	Name	Objekt	Feld 1	Wert 1	Feld 2	Wert 2
Transaktion	SESSION_MANAGER	S_TCODE	TCD	STUSOBTRACE		
Transaktion	SESSION_MANAGER	S_TCODE	TCD	Z_T000		
Transaktion	SM30	S_ADMI_FCD	S_ADMI_FCD	T000		
Transaktion	SM30	S_CTS_ADAMI	CTS_ADMFCT	TABL		
Transaktion	SM30	S_TABU_CLI	CLIIDMAINT	X		
Transaktion	SM30	S_TABU_DIS	DICBERCLS	SS	ACTVT	02
Transaktion	SM30	S_TABU_DIS	DICBERCLS	SS	ACTVT	03
Transaktion	SM30	S_TABU_NAM	ACTVT	02	TABLE	T000
Transaktion	SM30	S_TABU_NAM	ACTVT	03	TABLE	T000
Transaktion	SM30	S_TCODE	TCD	SCC4		
Transaktion	STUSOBTRACE	S_ADMI_FCD	S_ADMI_FCD	STOR		
Transaktion	STUSOBTRACE	S_ALV_LAYO	ACTVT	23		
Transaktion	STUSOBTRACE	S_ALV_LAYR	ACTVT	23	REPORT	RSU22_USOB_AUTHVALTRC_DISPLAY
Transaktion	STUSOBTRACE	S_GUI	ACTVT	61		
Transaktion	STUSOBTRACE	S_GUI	ACTVT	61		
Transaktion	STUSOBTRACE	S_TCODE	TCD	STUSOBTRACE		
Transaktion	Z_T000	S_ADMI_FCD	S_ADMI_FCD	T000		
Transaktion	Z_T000	S_CTS_ADAMI	CTS_ADMFCT	TABL		
Transaktion	Z_T000	S_TABU_CLI	CLIIDMAINT	X		
Transaktion	Z_T000	S_TABU_DIS	DICBERCLS	SS	ACTVT	02
Transaktion	Z_T000	S_TABU_DIS	DICBERCLS	SS	ACTVT	03
Transaktion	Z_T000	S_TABU_NAM	ACTVT	02	TABLE	T000
Transaktion	Z_T000	S_TABU_NAM	ACTVT	03	TABLE	T000
Transaktion	Z_T000	S_TCODE	TCD	SCC4		
Transaktion	Z_T000	S_TCODE	TCD	Z_T000		

Abbildung 7.13 Auswertung des Berechtigungstrace

Starten Sie danach die Transaktion SU24 (Berechtigungs-vorschlagspflege). In Abbildung 7.14 fällt im Bereich ❶ auf, dass keine Objekte enthalten sind. Sie erhalten den Hinweis ZU IHRER SELEKTION EXISTIEREN KEINE BERECHTIGUNGSOBJEKTZUORDNUNGEN ❷. Dieser Hinweis bedeutet, dass es entweder keine Daten in der Transaktion SU22 gibt oder (der Regelfall) dass eine Übernahme noch nicht erfolgt ist. Der Button BERECHTIGUNGSTRACE: EIN ❸ zeigt an, dass der Berechtigungs-trace aktuell eingeschaltet ist. Durch einen Klick auf den Button SAP-DATEN ❹ können Sie die Übernahme der SAP-Daten starten. Sind keine SAP-Daten gepflegt, können Sie die Werte aus dem Berechtigungs-trace durch einen Klick auf OBJEKT • OBJEKTE AUS BERECHTIGUNGSTRACE EINFÜGEN • LOKAL einfügen.

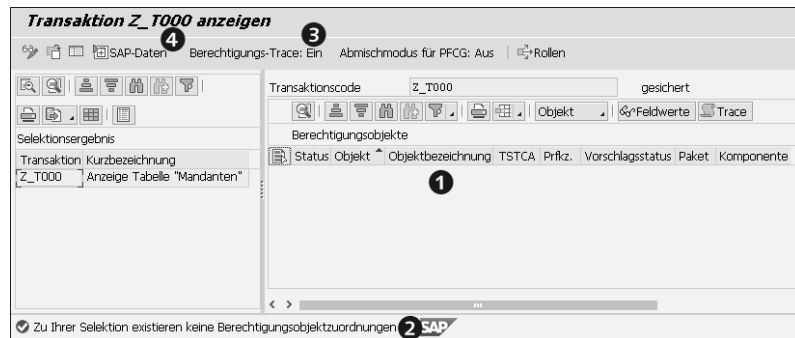


Abbildung 7.14 Werte für die kundeneigene Transaktion SU24 vor Übernahme der SAP-Daten

### Berechtigungs-trace für Berechtigungs-vorschlagswerte und Rollenpflege

Die Werte des Berechtigungs-trace stehen Ihnen auch in der Rollenpflege (Berechtigungen) zur Verfügung, siehe Abschnitt 6.6, »Vom Trace zur Rolle«.

Nach der Übernahme der SAP-Daten bzw. der Berechtigungsobjekte aus dem Berechtigungs-trace sehen Sie die aufgezeichneten Objekte im Status UNGEPFLEGT (siehe Abbildung 7.15 ❶). Nun können Sie auf alle Tracewerte ❷ zur Pflege zugreifen, um die Berechtigungs-vorschlagswerte auszuprägen. Die Funktion der Übernahme der Tracewerte ist vergleichbar mit dem in Abschnitt 6.6 dargestellten Verfahren.

Status	Objekt	Objektbezeichnung	TSTCA	Prifz.	Vorschlag	SAP-Prifz.	SAP-Vrsch.	Sync.	Paket	Komponente
UNGEPFLEGT	S_ADMI_FCD	Systemberechtigungen		prüfen					SUSR	BC-SEC-USR-ADM
UNGEPFLEGT	S_CTS_ADMI	Administrationsfunktionen im Change & Transport System		prüfen					SCTS_BAS	BC-CTS-ORG
UNGEPFLEGT	S_TABU_CLI	Tabellenpflege mandantenunabhängiger Tabellen		prüfen					SVIM	BC-CUS-TOL-TME
UNGEPFLEGT	S_TABU_DIS	Tabellenpflege (über Standardtools wie zB SM30)		prüfen					SVIM	BC-CUS-TOL-TME
UNGEPFLEGT	S_TABU_NAM	Tabellenzugriff über generische Standardtools		prüfen					SVIM	BC-CUS-TOL-TME
UNGEPFLEGT	S_TCODE	Transaktionscode-Prüfung bei Transaktionsstart		prüfen	Nein				SVUR	BC-SEC-USR-ADM

Abbildung 7.15 Werte für kundeneigene Transaktion SU24 nach der Übernahme der SAP-Daten bzw. der Daten aus dem Berechtigungs-trace

## 7.2.2 Vorgehen beim Systemtrace

Um den Systemtrace zu nutzen, stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Wie Sie den Systemtrace aus der Auswertung in der Rollen- und Vorschlagswertpflege starten, sehen Sie in Abbildung 7.16. Sie können den Systemtrace aus folgenden Funktionen dieses Kontextes heraus starten:

- ▶ Transaktion PFCG (Pflege von Rollen) • Registerkarte MENÜ • Button ÜBERNAHME VON MENÜS • Menüeintrag IMPORT AUS TRACE
- ▶ Transaktion PFCG (Pflege von Rollen) • Registerkarte BERECHTIGUNGEN • Bereich BERECHTIGUNGS-DATEN PFLEGEN UND PROFILE GENERIEREN • Folgebildschirm • Button TRACE
- ▶ Transaktion SU24 (Berechtigungs-vorschlagspflege) • Button TRACE • Folgebildschirm • Button TRACE AUSWERTEN

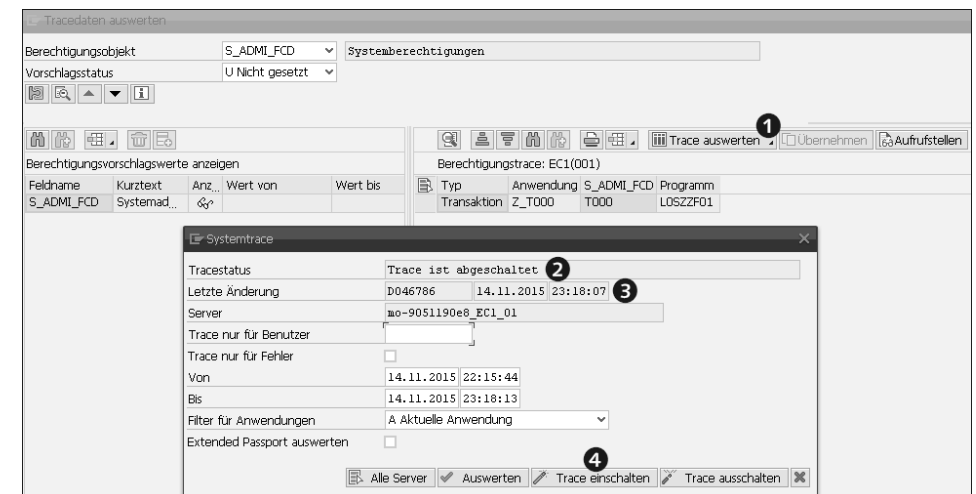


Abbildung 7.16 Trace aus der Auswertung in der Rollen- und Vorschlagswertpflege starten



Klicken Sie auf den Button TRACE AUSWERTEN (1 in Abbildung 7.16). Sie erhalten die Info, ob der Systemtrace ein- oder ausgeschaltet ist (2), wer der letzte Änderer war und wann die Änderung stattgefunden hat (3), schließlich klicken Sie auf den Button TRACE EINSCHALTEN (4), der den Trace startet.

Neben diesen Optionen steht Ihnen der Zugang über die Transaktion ST01 (Systemtrace) sowie über die Transaktion STAUTHTRACE (Berechtigungstrace) zur Verfügung.

### 7.2.3 Vorgehen beim Benutzertrace

Den Benutzertrace aktivieren Sie über den Profilparameter auth/auth\_user\_trace. Wie Sie Profilparameter pflegen, haben wir bereits in Abschnitt 7.2.1, »Vorgehen beim Berechtigungstrace«, beschrieben. Setzen Sie den Wert des Profilparameters auf Y (aktiv) oder F (aktiv mit Filter) (siehe Abbildung 7.11), diese Einstellungen können Sie auch dynamisch setzen. Den Filter setzen Sie, wie oben beschrieben, in der Transaktion STUSERTRACE entsprechend Ihren Anforderungen. Die Ergebnisse des Benutzertrace können Sie ebenfalls in dieser Transaktion über einen Klick auf den Button AUSWERTEN einsehen (siehe Abbildung 7.17).



Abbildung 7.17 Einstellungen des Filters für den Benutzertrace über Transaktion STUSERTRACE

Die Auswertung (siehe Abbildung 7.18) zeigt nun alle ausgeführten Anwendungen und die darin erfolgten Berechtigungsprüfungen mit Objekt und Feldwerten an. Im Gegensatz zum Berechtigungstrace können Sie bei der Auswertung auf einen bestimmten Benutzer filtern, und die Benutzer sind in der Liste enthalten. Diese Informationen können Sie nun nutzen, um Berechtigungsvorschlagswerte oder Rollen zu pflegen.

Benutzertrace für Berechtigungsprüfungen: 23 Treffer											
Typ der Anwendung	Name der Anwendung	Benutzer	Ergebnis	Objekt	Feld 1	Wert 1	Feld 2	Wert 2	Datum	Zeit	
RFC-Funktionsbaustein	MENU_GENERATE_SAP_MENU	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_RFC	RFC_TYPE	FLGR	RFC_NAME	*	14.02.2016	22:40:01	
Transaktion	PFCG	SAP_PRESS	Berechtigungsprüfung erfolgreich	PLOG	PLVAR	01	OTYPE	AG	14.02.2016	22:39:51	
Transaktion	PFCG	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_AGR	ACT_GROUP	MMM_PXXXX_PURCHASING-ORDER_N	ACTVT	02	14.02.2016	22:39:50	
Transaktion	PFCG	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_SAS	ACTVT	22	CLASS		14.02.2016	22:39:51	
Transaktion	RZ11	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ADMI_FCD	S_ADMI_FCD	PADM			14.02.2016	22:36:18	
Transaktion	RZ11	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ADMI_FCD	S_ADMI_FCD	PADM			14.02.2016	22:36:53	
Transaktion	SESSION_MANAGER	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_TCODE	TCD	PFCG			14.02.2016	22:39:45	
Transaktion	SESSION_MANAGER	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_TCODE	TCD	STUSERTRACE			14.02.2016	22:36:26	
Transaktion	SESSION_MANAGER	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_TCODE	TCD	SU01			14.02.2016	22:39:01	
Transaktion	SESSION_MANAGER	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_AGR	ACT_GROUP		ACTVT		14.02.2016	22:39:45	
Transaktion	SESSION_MANAGER	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_GRP	CLASS		ACTVT		14.02.2016	22:39:01	
Transaktion	STUSERTRACE	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ADMI_FCD	S_ADMI_FCD	STUR			14.02.2016	22:40:16	
Transaktion	STUSERTRACE	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ADMI_FCD	S_ADMI_FCD	STUR			14.02.2016	22:36:26	
Transaktion	STUSERTRACE	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ALV_LAYO	ACTVT	23			14.02.2016	22:40:16	
Transaktion	STUSERTRACE	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_GUI	ACTVT	61			14.02.2016	22:40:16	
Transaktion	STUSERTRACE	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ALV_LAYO	ACTVT	61			14.02.2016	22:39:13	
Transaktion	SU01	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_GUI	ACTVT	61			14.02.2016	22:39:13	
Transaktion	SU01	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_GRP	CLASS		ACTVT	02	14.02.2016	22:39:07	
Transaktion	SU01	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_SAS	ACTVT	22	CLASS		14.02.2016	22:39:12	
Transaktion	SU01	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_SAS	ACTVT	22	CLASS		14.02.2016	22:39:34	
Transaktion	SU01	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_SAS	ACTVT	22	CLASS		14.02.2016	22:39:34	

Abbildung 7.18 Auswertung des Benutzertrace über Transaktion STUSERTRACE

## 7.3 Upgrade-Nacharbeiten von Berechtigungen

Mit den Basisreleases 7.31 und 7.40 sind eine Reihe von Änderungen im Upgrade-Tool für den Profilgenerator vollzogen worden. Des Weiteren wurde die Dokumentationslage verbessert, die nun die Wartung von Berechtigungsvorschlagswerten und Rollen im Upgrade und beim Einspielen von Support Packages vereinfacht. Wir haben aktuelle SAP-Hinweise dazu in Tabelle 7.8 zusammengestellt.

SAP-Hinweis	Kurztext	Release
1539556	FAQ Administration von Berechtigungsvorschlagswerten	releaseunabhängig
1599128	SU25 – Optimierung der Upgrade-Nachbereitung	SAP_BASIS 70 700–702 SAP_BASIS 71 710– 30 SAP_BASIS 731

Tabelle 7.8 SAP-Hinweise zum Upgrade von Berechtigungen

SAP-Hinweis	Kurztext	Release
1696484	SU25 – Behandlung kundeneigener Berechtigungsvorschlagswerte	SAP_BASIS 70 700–702 SAP_BASIS 71 710–730
1691993	SU2X – Optimierung der Berechtigungsvorschlagswertepflege	SAP_BASIS 70 700–702 SAP_BASIS 71 710–730 SAP_BASIS 731

Tabelle 7.8 SAP-Hinweise zum Upgrade von Berechtigungen (Forts.)

Die folgenden Ausführungen und Screenshots beziehen sich auf SAP\_BASIS 7.40, allerdings sind die meisten Funktionen auch in früheren Releases enthalten.

Die Transaktion SU25 (Upgrade-Tool für den Profilgenerator) dient dem initialen Befüllen der Kundentabellen zum ersten Einsatz des Profilgenerators und dazu, die Kundentabellen in einem Upgrade auf den neuesten Stand zu bringen. Insgesamt stehen in der Transaktion SU25 folgende Schritte zur Verfügung (siehe Abbildung 7.19):

- ▶ Schritt 1 bereitet den Profilgenerator auf seine erste Verwendung vor, und die Kundentabellen werden initial befüllt. Mit Hinweis 1691993 (SU2X – Optimierung der Berechtigungsvorschlagswertepflege) ist dieser Schritt so verändert worden, dass ein zufälliges Überschreiben bereits gefüllter Kundentabellen und somit die Vernichtung kundeneigener Daten erschwert wird. Mehr dazu erfahren Sie in diesem Hinweis. Durch diese neue Funktion verändert sich die Anzeige der Transaktion SU25 (Upgrade-Tool für den Profilgenerator) in Schritt 1 dann, wenn Schritt 2a bereits einmal im System ausgeführt wurde. Die neue Darstellung ist in Abbildung 7.19 unter KUNDENTABELLEN WURDEN INITIAL BEFÜLLT ZU sehen.
- ▶ Die Schritte 2a–2d sind für das Upgrade selbst erforderlich.
- ▶ Schritt 3 dient dem Transport der durch die vorangegangenen Schritte geänderten Kundenvorschlagswerttabellen. Beachten Sie, dass nur diese transportiert werden.
- ▶ Schritt 4 ist ein Absprung in die Transaktion SU24 (Berechtigungsobjektprüfungen unter Transaktionen).
- ▶ Schritt 5 ermöglicht das globale Deaktivieren von Berechtigungsprüfungen.

Durchzuführende Aktionen	Datum	Uhrzeit	Benutzer
Installation des Profilgenerators			
1. Kundentabellen wurden initial befüllt	24.09.2014	11:46:06	
Nachbearbeiten der Einstellungen nach Upgrade auf ein höheres Release			
2a. Automatischer Abgleich mit SU22-Daten	08.07.2015	13:54:53	
2b. Modifikationsabgleich mit SU22-Daten	07.08.2014	16:52:41	
2c. Zu überprüfende Rollen	17.09.2015	11:03:45	
2d. Veränderte Transaktionscodes anzeigen	01.10.2014	15:34:20	
Transportanschluß			
3. Transport der Kundentabellen	01.09.2015	15:32:30	
Anpassung der Berechtigungsprüfungen(optional)			
4. Prüfkennzeichen in Anwendungen (SU24)	05.04.2014	11:27:41	
5. Berechtigungsobjekte global ausschalten	10.11.2015	13:15:40	
Transaktionsstartberechtigungsprüfung (SE97)	10.06.2013	08:03:55	
Abgleich schaltbarer Berechtigungsprüfungen (SACF)	15.10.2015	15:53:16	
Abgleich generischer Whitelisten (SLDW)	07.01.2015	10:38:54	
Manuelle Anpassung ausgewählter Rollen			
Erzeugen von Rollen aus manuell erstellten Profilen	05.04.2014	18:18:36	
Standardrolle SAP_NEW generieren	15.06.2015	15:01:29	
Standardrolle SAP_APP generieren	26.08.2015	14:22:58	
Allgemeine Wartung für Vorschlagswerte			
Bereinigung der Applikationsheaderdaten			
Konsistenzprüfung für Vorschlagswerte	29.07.2015	19:28:47	

Abbildung 7.19 Upgrade-Tool für den Profilgenerator

Dargestellt wird nun das Upgrade, also das Nachbearbeiten der Einstellungen nach dem Upgrade auf ein höheres Release. Dieses wird in den Schritten 2a–2d vollzogen.

Zunächst wird in Schritt 2a der Abgleich der Vorschlagswerte ausgeführt. Dieser Schritt ist zwingend erforderlich. Dabei werden die neuen Berechtigungsvorschlagswerte (also die Werte nach Upgrade oder Einspielen eines Support Packages) in die Kundentabellen übernommen.

Schritt 2a:  
Vorbereitung –  
Abgleich mit  
SAP-Werten

Verwenden Sie dafür am besten den EXPERTENMODUS FÜR SCHRITT 2, indem Sie auf den gleichnamigen Button klicken. Dabei können Sie (ab Basisrelease 7.00) wählen, ob Sie einen Abgleich der SAP-Standardanwendungen oder einen Abgleich von kundeneigenen und Partneranwendungen der neu ausgelieferten Werte mit Ihren kundenspezifischen Werten vornehmen möchten, wie es in Abbildung 7.20 gezeigt wird.

Die Übersicht in Abbildung 7.21 zeigt, welche Anwendungen abzugleichen sind und bei welchen Anwendungen ein manueller Abgleich notwendig ist. Ein manueller Abgleich ist erforderlich, wenn Daten in der Transaktion SU24 für diese Anwendung im Vorfeld geändert worden sind und Sie entscheiden müssen, ob diese Änderungen übernommen werden oder ob die aktuellen Standardwerte aus der Transaktion SU22 übernommen werden sollen.

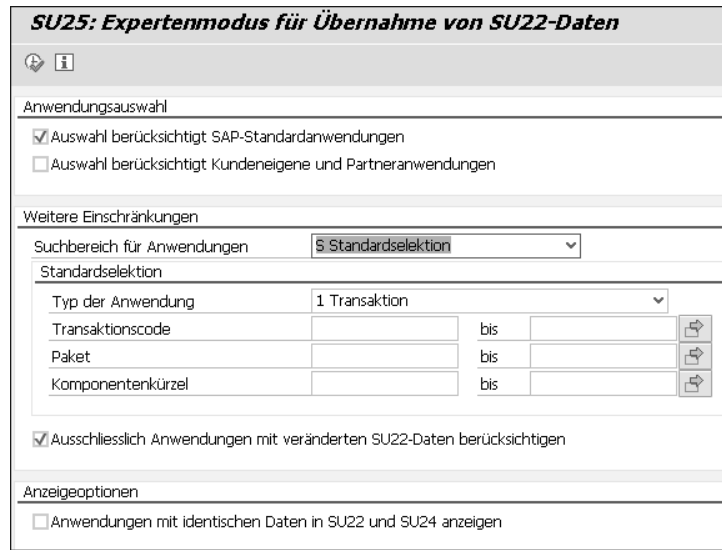


Abbildung 7.20 Auswahl des Abgleichs bei Upgrade-Nacharbeiten unter Verwendung des Expertenmodus für Schritt 2



Abbildung 7.21 Übernahmeoptionen von Anwendungen in Schritt 2a

Die Werte, die in der »alten« Kundentabelle kundenseitig gepflegt wurden, werden gekennzeichnet, um sie in Schritt 2b manuell überprüfen zu können. Dabei markieren Sie die Anwendungen, die Sie manuell abgleichen möchten, und klicken auf den Button MANUELLER ABGLEICH.

Schritt 2b:  
Abgleich  
betroffener  
Transaktionen

Änderungen an Prüfkennzeichen oder Feldwerten werden in diesem Schritt mit den neuen SAP-Vorschlägen verglichen. In Abbildung 7.22 ist der Bereich mit ❶ gekennzeichnet, in dem die Transaktionen enthalten sind, die von den aktuellen Standardvorschlägen abweichen. Die Einstellungen, die wir in Abschnitt 7.1.1, »Grundzustand und Pflege der Berechtigungsvorschlagswerte«, in Bezug auf die

Transaktion Anzeigen einer Bestellung vorgenommen haben, werden entsprechend nach dem Abgleich in Schritt 2a in Schritt 2b zur Bearbeitung angeboten. Sie sehen in Abbildung 7.22, dass die mit ❷ gekennzeichnete Änderung des Prüfkennzeichens dazu führt, dass der neue SAP-Vorschlag angezeigt wird. Ebenso ist es mit der durch ❸ gekennzeichneten Änderung des Vorschlags. Diese Änderungen erkennen Sie daran, dass in der Spalte SYNC. die Buttons SAP-DATEN KOPIEREN zu sehen sind ❹. Durch einen Klick auf diese Buttons kopieren Sie den SAP-Vorschlag und überschreiben Ihre Kundenvorschlagswerte. Mit ❺ sind Änderungen der Feldwertvorschläge gekennzeichnet. Sie können die jeweiligen Werte nachpflegen. Im Bereich ❶ können Sie bestätigen, dass Sie die Prüfung vorgenommen haben, oder die gesamten restlichen Werte übernehmen. Davon raten wir Ihnen jedoch ab, sofern Sie regelmäßig und genau Ihre kundeneigenen Vorschläge ergänzt oder geändert haben.

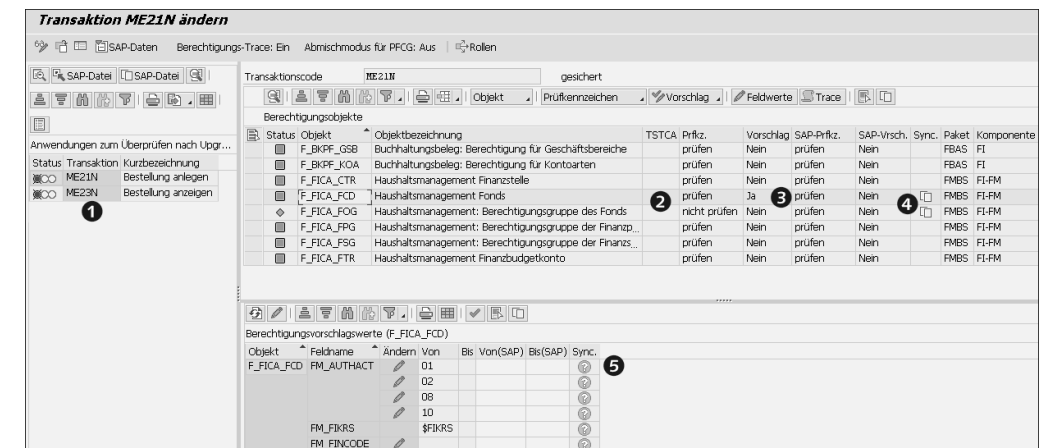


Abbildung 7.22 Berechtigungsvorschläge in Schritt 2b der Upgrade-Nacharbeiten

Die Systematik zur Pflege der Berechtigungsvorschlagswerte entspricht im Wesentlichen der Systematik, wie wir sie in Abschnitt 7.1.1, »Grundzustand und Pflege der Berechtigungsvorschlagswerte«, im Hinblick auf die Berechtigungsvorschlagswerte entwickelt haben.

Sofern Sie kundeneigene Organisationsebenen nutzen (siehe Abschnitt 7.8, »Anhebung eines Berechtigungsfeldes zur Organisationsebene«), sollten Sie den Report PFCG\_ORGFELD\_UPGRADE (Anpassung nach Upgrade für neue Org.-Ebenen) ausführen. Dadurch

Nacharbeit  
Schritt 2b:  
Kundeneigene  
Organisationsebenen

werden alle neuen Berechtigungsvorschlagsdaten, die SAP zu neuen Transaktionen ausgeliefert hat, auf die neuen Organisationsebenenfelder umgestellt. Der Report arbeitet mandantenunabhängig (SAP-Hinweis 323817).

Schritt 2c:  
Zu überprüfende  
Rollen

In diesem Schritt findet die Nachbearbeitung der durch das Upgrade betroffenen Rollen statt. Diese werden, wie in Abbildung 7.23 zu sehen ist, vorgeschlagen; dabei markiert eine rote Ampel (links in der jeweiligen Ampel) Pflegebedarf und eine grüne (rechts in der jeweiligen Ampel), dass keine Pflege (mehr) erforderlich ist.

Anzeige zu bearbeitender Rollen nach Vorschlagswertänderung		
Release / System-Id / Mandant:	751 / Y13 / 322	
Ausgeführt durch:	BONITZ	
Ausgeführt am:	21.11.2015/22:16:10	
Prüfe geänderte SU24-Daten ab dem:	18.11.2015	
Die angezeigten Rollen enthalten Applikationen, deren Berechtigungsvorschläge sich geändert haben. Folgende Status treten auf:		
Rot (6 Rollen): Abmischen der Berechtigungsdaten notwendig und möglich (Abmischmodus aktiv)		
Grün (2 Rollen): Berechtigungsdaten wurden bereits abgemischt.		
Status	Rolle	Kurzbeschreibung der Rolle
	MY_TEST	meine testrolle
	DMM_PDEZR_PURCHASINGORDER_N	Bestellungen Bearbeiten für das Orglevel-Set DEZR
	MMM_PXXX_PURCHASING-ORDER_N	Bestellungen Bearbeiten - Referenzrolle
	Z_BERECHTIGUNGEN_BC_SEC_USR	Ber. fuer Entw./Dev.Supporter im Bereich BC-SEC-USR*
	ZTI_SU01_SU10	

Abbildung 7.23 Rollenüberprüfung in Schritt 2c der Upgrade-Nacharbeiten

Um bei den bereits eingeführten Beispielen zu bleiben: In Abschnitt 6.3.2, »Rollenpflege«, haben wir die Rolle MMM\_PXXXX\_PURCHASINGORDER\_N angelegt und daraus Rollen abgeleitet. Diesen Rollen ist die Transaktion ME21N (Bestellung anlegen) zugeordnet, die ebenfalls im Rahmen des Abschnitt 7.1.1, »Grundzustand und Pflege der Berechtigungsvorschlagswerte«, gepflegt wurde und nun von dem Upgrade betroffen ist.

Abbildung 7.24 zeigt, dass das ergänzte Berechtigungsobjekt erkannt und vorgeschlagen wurde. Da der Vorschlag nur das Feld AKTIVITÄT BERECHTIGUNGSPRÜFUNG betraf und das Feld FINANZKREIS eine Organisationsebene ist, verbleibt nur das Feld FONDS, das manuell gepflegt werden muss. Die Änderung der Referenzrolle wird durch den Button ABGELEITETE ROLLEN GENERIEREN automatisch mit gepflegt.

Rolle ändern: Berechtigungen					
Rolle: MMM_PXXXX_PURCHASING-ORDER_N					
Pflege: 3 ungepflegte Orgebenen, 2 offene Felder					
Status: geändert					
Gruppe/Objekt/Berechtigung/Feld	Pflegestatus	Aktualisier...	Aktion	Wert	Text
Objektklasse AAAB	Standard	Aktualisiert			Anwendungsübergreifende Berechtigungsobjekte
Objektklasse FI	Standard	Neu			Finanzwesen
Berechtigungsobjekt F_FICA_FCD	Standard	Neu			Haushaltsmanagement Fonds
Berechtigung T-E118117500	Standard	Neu			Haushaltsmanagement Fonds
FM_AUTHACT	Standard			01, 02, 08, 10	Aktivität Berechtigungsprüfung
FM_FIKRS (\$FIKRS)	Standard			\$FIKRS	Finanzkreis
FM_FINCODE	Standard				Fonds
Objektklasse MM_E	Gepflegt	Neu			Materialwirtschaft - Einkauf

Abbildung 7.24 Rollenänderung in Schritt 2c der Upgrade-Nacharbeiten

In der Hilfe zu diesem Schritt wird von SAP folgende alternative Vorgehensweise vorgeschlagen:

SAP-Alternativ-  
vorschlag

*Alternativ können Sie auch auf eine Nachbearbeitung der Rollen verzichten und allen Benutzern zunächst die Rolle SAP\_NEW generieren und manuell zuordnen (siehe dazu SAP-Hinweis 1711620) [...] Die Rollen behalten dann den Status »Profilabgleich erforderlich« und können bei der nächsten notwendigen Änderung – z. B. wenn das Menü der Rolle geändert wird – angepasst werden. Bei Verwendung von sehr vielen Rollen kann dieses Verfahren sinnvoll sein. Sie haben dann Zeit, die Rollen nach und nach anzupassen. (Systemhilfe)*

Dieser Vorschlag birgt erhebliche Risiken, vor allem in den Fällen, in denen neue Funktionen, neue Berechtigungsprüfungen oder neue Differenzierungspotenziale bereitgestellt und genutzt werden. Die selbst generierte Rolle SAP\_NEW (siehe SAP-Hinweis 1711620) enthält alle neuen Berechtigungen für das neue Release. Damit wird durch ein derartiges Vorgehen gegen das Prinzip verstoßen, dass nur die Berechtigungen vergeben werden, die für die Ausführung einer definierten Tätigkeit des Benutzers erforderlich sind. Für die Zeit der Nutzung der Rolle SAP\_NEW ist davon auszugehen, dass die Berechtigungen nicht regelkonform sind. Der Gegenbeweis wäre nur durch eine Risikoanalyse – basierend auf den alten und neuen Prüfungen – anzutreten.

#### Einfaches Upgrade

Die Nutzung eines gewissenhaft eingehaltenen Ableitungskonzepts, stetig gepflegter Berechtigungsvorschlagswerte und des Upgrade-Tools führt zu einem einfachen Upgrade im Bereich Berechtigungen. In diesem idea-

len Fall müssen im Wesentlichen nur die neuen Transaktionen, Berechtigungsobjekte und Vorschlagsänderungen bewertet und umgesetzt werden. Der Aufwand für das Upgrade sinkt mit der Genauigkeit der Standardeinhaltung.

**Empfehlung zum Aufwand**

Wir haben Upgrade-Projekte mit einem Aufwand für Berechtigungen zwischen 20 und 300 Beratertagen in Konzernstrukturen kennengelernt. Kommen Sie in der Abschätzung des Aufwands zu dem Ergebnis, dass mehr als 50 Tage Aufwand zu erwarten sind, empfiehlt es sich dringend, ein Redesign und die Rückkehr zum Standard zu prüfen. Das verursacht unter Umständen sofort einen geringeren Aufwand, als den Status quo anzuheben. Definitiv werden Ihre Kosten bereits mittelfristig deutlich sinken.

**Schritt 2d: Veränderte Transaktionscodes anzeigen**

In diesem Schritt findet ein Abgleich statt, welche Transaktionen durch neuere Transaktionen ersetzt werden könnten. Dieser Abgleich dient vor allem der Unterstützung der Prozessverantwortlichen. Diese müssen letztlich festlegen, welche Transaktionen wie zu nutzen sind. Sie sollten das Ergebnis des Abgleichs also den Prozessverantwortlichen übermitteln und diese die Festlegung treffen lassen.

Neue Transaktionen haben gegebenenfalls Auswirkungen auf die bestehenden Prozesse, aber auch auf die bestehenden Berechtigungen. Ein Beispiel für unter Umständen nicht gewollte Auswirkungen auf Berechtigungen ist die bereits diskutierte Enjoy-Transaktion (siehe Abschnitt 7.1.1) zur Bestellung, es kann auch aus Sicht von Berechtigungen Gründe geben, lieber weiterhin auch die alte Transaktion zu nutzen.

### 7.4 Parameter für Kennwortregeln

Die für das Login geltenden Kennwortregeln werden über Profilparameter gesetzt. Diese werden über die Transaktion RZ10 (Pflege der Profilparameter) gepflegt. Die Pflege der Profilparameter fällt in die Verantwortung der Basisadministration. Wir empfehlen Ihnen, die gewünschten Einstellungen Ihrer Basisadministration zu überlassen.

Die Auswertung der Profilparameter ist über den Report RSPARAM (Anzeige der SAP-Profilparameter) möglich (siehe Abbildung 7.25). Einige exemplarische Parameter sind in Tabelle 7.9 dargestellt.

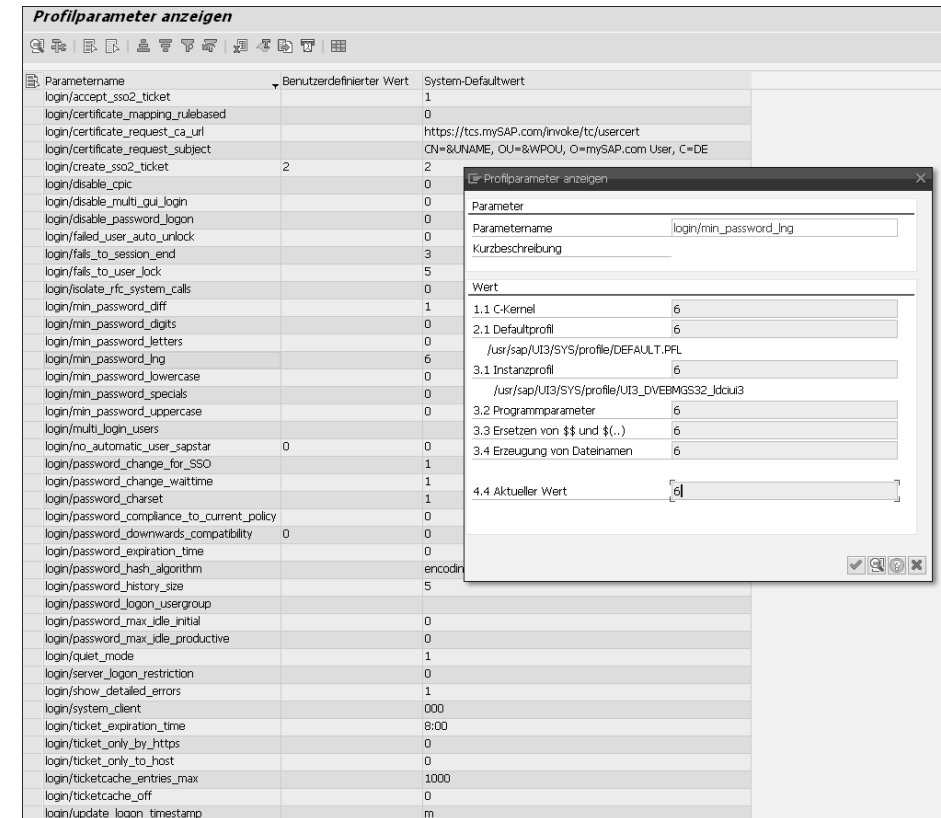


Abbildung 7.25 Anzeige der Profilparameter

Parameter	Beschreibung
login/accept_sso2_ticket	Um ein Single Sign-on (SSO) zwischen SAP-Systemen bzw. auch übergreifend zu Nicht-SAP-Systemen zu ermöglichen, können SSO-Tickets verwendet werden.
login/failed_user_auto_unlock	Kontrolliert die Entsperrung von durch Fehlmeldungen gesperrten Benutzern. Ist der Parameter auf 1 gesetzt, werden Sperren, die wegen fehlgeschlagener Kennwortanmeldeversuche gesetzt wurden, automatisch am nächsten Tag durch das System aufgehoben.
login/fails_to_session_end	Anzahl der Falschmeldungen, die mit einem Benutzerstamm gemacht werden können, bis das Anmeldeverfahren abgebrochen wird

Tabelle 7.9 Parameter für Kennwortregeln (Angaben aus der Systemdokumentation)

Parameter	Beschreibung
login/fails_to_user_lock	Bei jedem fehlerhaften Kennwortanmeldeversuch wird der Falschanmeldezähler für den betreffenden Benutzerstammsatz erhöht. Die Anmeldeversuche können im Security Audit Log protokolliert werden. Bei Überschreiten der durch diesen Parameter vorgegebenen Grenze wird der betreffende Benutzer gesperrt. Dieser Vorgang wird zusätzlich im Syslog protokolliert.
login/min_password_diff	Mit diesem Parameter kann der Administrator festlegen, in wie vielen Zeichen sich ein neues Kennwort vom alten Kennwort mindestens unterscheiden muss, wenn der Benutzer sein Kennwort ändert.
login/min_password_digits	Dieser Parameter bestimmt die minimale Anzahl von Ziffern (0–9), die im Kennwort enthalten sein müssen. Er wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen von Kennwörtern.
login/min_password_letters	Dieser Parameter bestimmt die minimale Anzahl von Buchstaben, die im Kennwort enthalten sein müssen. Er wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen von Kennwörtern.
login/min_password_lng	Der Parameter bestimmt die Minimallänge des Anmeldekennwortes. Das Kennwort muss mindestens drei Zeichen lang sein. Der Administrator kann aber auch eine größere Minimallänge festlegen. Diese Vorgabe wirkt sich sowohl bei der Vergabe neuer Kennwörter als auch beim Ändern oder Rücksetzen bestehender Kennwörter aus.
login/min_password_lowercase	Dieser Parameter bestimmt die minimale Anzahl von Kleinbuchstaben, die im Kennwort enthalten sein müssen. Er wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen von Kennwörtern. Dieser Parameter wird nicht ausgewertet, wenn der Profilparameter <code>login/password_downwards_compatibility</code> auf den Wert 5 gesetzt ist.

**Tabelle 7.9** Parameter für Kennwortregeln  
(Angaben aus der Systemdokumentation) (Forts.)

Parameter	Beschreibung
login/min_password_specials	Dieser Parameter bestimmt die minimale Anzahl von Sonderzeichen, die im Kennwort enthalten sein müssen. Er wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen von Kennwörtern.
login/min_password_uppercase	Dieser Parameter bestimmt die minimale Anzahl von Großbuchstaben, die im Kennwort enthalten sein müssen. Er wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen von Kennwörtern. Dieser Parameter wird nicht ausgewertet, wenn der Profilparameter <code>login/password_downwards_compatibility</code> auf den Wert 5 gesetzt ist.
login/password_change_waittime	Mit diesem Parameter kann festgelegt werden, nach welcher Zeitspanne (gemessen in Tagen) ein Benutzer sein Kennwort erneut ändern kann. Nur Kennwortänderungen, die der Benutzer veranlasst hat, werden in Betracht gezogen.
login/password_expiration_time	Gültigkeitsdauer von durch den Benutzer gesetzten Kennwörtern (in Tagen) bis zur nächsten Änderung. Die Berechnung erfolgt abhängig vom Datum der letzten Kennwortänderung.
login/password_max_idle_productive	maximale Zeitspanne (in Tagen) zwischen dem Zeitpunkt der letzten Anmeldung mit einem durch den Benutzer gesetzten Kennwort und der nächsten Anmeldung mit diesem Kennwort
login/password_max_idle_initial	maximale Zeitspanne (in Tagen) zwischen dem Zeitpunkt der Kennwort(rück)setzung, Initialkennwort durch den Administrator gesetzt, und der nächsten Anmeldung mit diesem Kennwort
login/password_history_size	Dieser Parameter regelt die Größe der Kennworthistorie. Die Kennworthistorie wird ausgewertet, wenn ein Benutzer ein neues Kennwort wählt: Das System lehnt die (Wieder-) Verwendung von Kennwörtern, die in der Kennworthistorie gespeichert sind, ab.

**Tabelle 7.9** Parameter für Kennwortregeln  
(Angaben aus der Systemdokumentation) (Forts.)

Bitte beachten Sie auch den SAP-Hinweis 2467 (Kennwortregeln und Vermeidung fehlerhafter Anmeldungen).

Verbotene Kennwörter in der Tabelle USR40

In der Tabelle USR40 (Tabelle für verbotene Kennwörter) können darüber hinaus »verbotene« Kennwörter hinterlegt werden. Dies ist sowohl als Muster »\*WORT\*, \*20??\*«, als auch als konkreter Wert »Mama« möglich. Da dies Auswirkungen auf die Performance hat, sollten Sie unbedingt über die genannten Parameter eine sinnvolle Password Policy erzwingen, in dieser Tabelle sollten Sie möglichst nur unmittelbar offensichtliche Werte eintragen, wie z. B. den Namen des Unternehmens.

Customizing-Parameter in der Tabelle PRGN\_CUST

Über die Customizing-Parameter in der Tabelle PRGN\_CUST wird der Kennwortgenerator in den Transaktionen SU01 und SU10 gesteuert. Eine Übersicht über diese Customizing-Parameter finden Sie in Tabelle 7.10. Die Werte der Profilparameter übersteuern die Einträge zu den Customizing-Parametern, damit keine ungültigen Kennwörter generiert werden. Sollte also der Wert eines Customizing-Parameters kleiner sein als der Wert des korrespondierenden Profilparameters, wird stattdessen der Standardwert des Customizing-Parameters gezogen. Analog verhält es sich, wenn kein Wert gepflegt wurde.

Parameter	Beschreibung
GEN_PSW_MAX_LENGTH	Legt die maximale Länge des generierten Passwortes fest.
GEN_PSW_MAX_LETTERS	Legt die maximale Anzahl an Buchstaben im generierten Passwort fest.
GEN_PSW_MAX_DIGITS	Legt die maximale Anzahl an Zahlen im generierten Passwort fest.
GEN_PSW_MAX_SPECIALS	Legt die maximale Anzahl an Sonderzeichen im generierten Passwort fest.

Tabelle 7.10 Parameter für die Kennwortgenerierung

Sicherheitsrichtlinien

Zusätzlich zu den globalen Einstellungen der Kennwortregeln können Sie ab Release SAP NetWeaver 7.31 Kennwortregeln auch individuell über Sicherheitsrichtlinien definieren. Sie ordnen einem Benutzer die jeweilige Sicherheitsrichtlinie über die Transaktion SU01 zu. Ist einem Benutzer eine Sicherheitsrichtlinie zugeordnet, überschreiben die Werte der Sicherheitsrichtlinie die global gültigen Kennwortregeln. Für Einstellungen, deren Parameter nicht in der Sicherheitsrichtlinie gepflegt wurden, oder Benutzer, denen keine Sicherheitsrichtlinie zugeordnet ist, bleiben die globalen Einstellun-

gen der Profilparameter weiterhin relevant. Sie definieren Sicherheitsrichtlinien über die Transaktion SECPOL; ein Beispiel haben wir in Abbildung 7.26 dargestellt und einige exemplarische Parameter sind in Tabelle 7.11 aufgeführt.

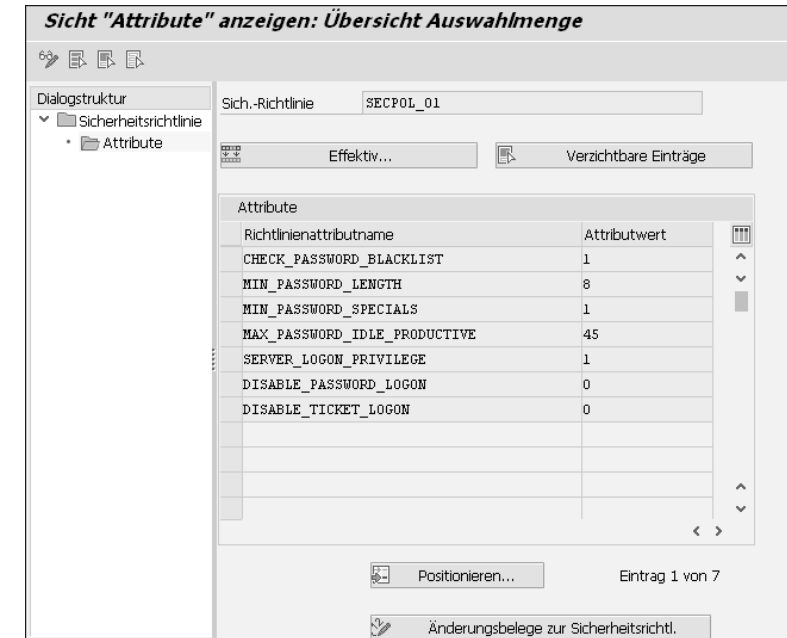


Abbildung 7.26 Definition einer Sicherheitsrichtlinie in der Transaktion SECPOL

Parameter	Beschreibung
DISABLE_TICKET_LOGON	Legt fest, ob sich ein Benutzer mit Anmelde- oder Zusicherungsticket am System anmelden kann.
MAX_FAILED_PASSWORD_LOGON_ATTEMPTS	Funktion analog zum Profilparameter login/fails_to_user_lock
MIN_PASSWORD_DIFFERENCE	Funktion analog zum Profilparameter login/min_password_diff
MIN_PASSWORD_DIGITS	Funktion analog zum Profilparameter login/min_password_digits
MIN_PASSWORD_LETTERS	Funktion analog zum Profilparameter login/min_password_letters
MIN_PASSWORD_LENGTH	Funktion analog zum Profilparameter login/min_password_lng

Tabelle 7.11 Parameter der Sicherheitsrichtlinien

Parameter	Beschreibung
PASSWORD_CHANGE_INTERVAL	Funktion analog zum Profilparameter <code>login/password_expiration_time</code>
CHECK_PASSWORD_BLACKLIST	Prüft bei der Eingabe des Kennwortes gegen die Negativliste verbotener Kennwörter (es werden die Einträge in der Tabelle USR40 geprüft).
SERVER_LOGON_PRIVILEGE	Legt fest, ob sich ein Benutzer trotz gesetzter Zugriffsbeschränkung für einen Server an diesem anmelden kann. Über den Profilparameter <code>login/server_logon_restriction</code> können Sie so eine Zugriffsbeschränkung setzen.

Tabelle 7.11 Parameter der Sicherheitsrichtlinien (Forts.)

Mit der Einführung der Sicherheitsrichtlinien gelten nun auch die Regeln zu den Inhalten der Kennwörter für Benutzer vom Typ System und Service. Regeln für die Änderung von Kennwörtern sind weiterhin nicht für diese Benutzertypen gültig. Diese Änderung ist erfolgt, da es Ihnen nun möglich ist, für diese Benutzer eigene Sicherheitsrichtlinien zu definieren und so z. B. sicherzustellen, dass weiterhin abwärtskompatible Passwörter für diese Benutzer verwendet werden.

## 7.5 Menükonzept

Ein Menükonzept wird häufig verwendet, um den Endbenutzern übersichtliche Benutzermenüs anzubieten. Das Menükonzept bedeutet keine Einschränkung von Berechtigungen. Im Folgenden werden wir Ihnen einen einfachen Vorschlag machen, wie ein Menükonzept aussehen kann. Dabei gehen wir davon aus, dass Sie entweder das »alte« Bereichsmenü (Transaktion SE43) oder Menüvorlagen, die in nicht weiter ausgeprägten Rollen vorgehalten werden, als Schablone für das Rollenmenü nutzen. Darüber hinaus empfehlen wir lediglich, alle Rollenmenüs auf Basis dieser Schablonen einzurichten.

**Präferenzen für Menüs** Die einzige dringende Anforderung, die an ein Menükonzept zu stellen ist, ist die, dass es logisch konsistent sein muss. Ob ein Menükonzept für Ihre Organisation sinnvoll ist und ob Sie Ihr Menü auf Standard-,



## Auf einen Blick

1	Einleitung .....	27
<b>TEIL I Betriebswirtschaftliche Konzeption</b>		
2	Einführung und Begriffsdefinition .....	35
3	Organisation und Berechtigungen .....	67
4	Rechtlicher Rahmen – normativer Rahmen .....	113
5	Berechtigungen in der Prozesssicht .....	143
<b>TEIL II Werkzeuge und Berechtigungspflege im SAP-System</b>		
6	Technische Grundlagen der Berechtigungspflege .....	163
7	Systemeinstellungen und Customizing .....	241
8	Rollenzuordnung über das Organisationsmanagement .....	331
9	Zentrales Management von Benutzern und Berechtigungen .....	341
10	Berechtigungen: Standards und Analyse .....	387
11	SAP Access Control .....	419
12	User Management Engine .....	437
<b>TEIL III Berechtigungen in spezifischen SAP-Lösungen</b>		
13	Berechtigungen in SAP ERP HCM .....	461
14	Berechtigungen in SAP CRM .....	487
15	Berechtigungen in SAP SRM .....	565
16	Berechtigungen in SAP BW .....	589
17	Berechtigungen in der SAP-BusinessObjects-Business-Intelligence-Plattform 4.x .....	615
18	RFC-Sicherheit mittels Unified Connectivity .....	631
19	Berechtigungen in SAP HANA .....	649
20	Berechtigungen in SAP S/4HANA .....	669
21	SAP Business Suite: Prozesse und Einstellungen .....	679
22	Konzepte und Vorgehen im Projekt .....	759

# Inhalt

Vorwort .....	21
Danksagung .....	23

## **1** Einleitung ..... 27

### **TEIL I Betriebswirtschaftliche Konzeption**

## **2** Einführung und Begriffsdefinition ..... 35

2.1	Methodische Überlegungen .....	36
2.1.1	Ansätze für das betriebswirtschaftliche Berechtigungskonzept .....	37
2.1.2	Beteiligte am Berechtigungskonzept .....	39
2.2	Compliance ist Regelkonformität .....	40
2.3	Risiko .....	41
2.4	Corporate Governance .....	45
2.5	Technische vs. betriebswirtschaftliche Bedeutung des Berechtigungskonzepts .....	47
2.6	Technische vs. betriebswirtschaftliche Rolle .....	49
2.7	Beschreibung von Berechtigungskonzepten .....	51
2.7.1	Role Based Access Control .....	51
2.7.2	Core RBAC und SAP ERP .....	54
2.7.3	Hierarchical RBAC und SAP ERP – limitierte Rollenhierarchien .....	60
2.7.4	Hierarchical RBAC und SAP – allgemeine Rollenhierarchien .....	60
2.7.5	Constrained RBAC .....	61
2.7.6	Constrained RBAC und SAP ERP .....	63
2.7.7	Restriktionen des RBAC-Standards .....	64
2.7.8	Beschreibung technischer Berechtigungskonzepte .....	65

## **3** Organisation und Berechtigungen ..... 67

3.1	Organisatorische Differenzierung am Beispiel .....	69
3.2	Begriff der Organisation .....	71
3.3	Institutioneller Organisationsbegriff .....	72

3.4	Instrumenteller Organisationsbegriff .....	76
3.4.1	Aufbauorganisation .....	77
3.4.2	Aufgabenanalyse .....	85
3.5	Folgerungen aus der Organisationsbetrachtung .....	90
3.6	Die Grenzen der Organisation und das Internet der Dinge .....	91
3.7	Sichten der Aufbauorganisation in SAP-Systemen ....	92
3.7.1	Organisationsmanagement .....	93
3.7.2	Organisationssicht des externen Rechnungswesens .....	95
3.7.3	Organisationssicht des Haushaltsmanagements .....	96
3.7.4	Organisationssicht der Kostenstellenstandardhierarchie .....	97
3.7.5	Organisationssicht der Profit-Center- Hierarchie .....	97
3.7.6	Unternehmensorganisation .....	98
3.7.7	Organisationssicht im Projektsystem .....	99
3.7.8	Logistische Organisationssicht .....	100
3.7.9	Integration der Organisationssichten im Berechtigungskonzept .....	100
3.8	Organisationsebenen und -strukturen in der SAP Business Suite .....	101
3.8.1	Organisationsebene »Mandant« .....	102
3.8.2	Relevante Organisationsebenen des Rechnungswesens .....	103
3.8.3	Relevante Organisationsebenen in der Materialwirtschaft .....	107
3.8.4	Relevante Organisationsebenen im Vertrieb .....	108
3.8.5	Relevante Organisationsebenen in der Lagerverwaltung .....	108
3.8.6	Integration der Organisationsebenen im Berechtigungskonzept .....	108
3.9	Hinweise zur Methodik im Projekt .....	110
3.10	Fazit .....	112
<b>4</b>	<b>Rechtlicher Rahmen – normativer Rahmen .....</b>	<b>113</b>
4.1	Interne und externe Regelungsgrundlagen .....	114
4.2	Internes Kontrollsystem .....	118

4.3	Rechtsquellen des externen Rechnungswesens .....	120
4.3.1	Rechtsquellen und Auswirkungen für den privaten Sektor .....	121
4.3.2	Konkrete Anforderungen an das Berechtigungskonzept .....	124
4.4	Datenschutzrecht .....	124
4.4.1	Gesetzliche Definitionen in Bezug auf die Datenverarbeitung .....	128
4.4.2	Rechte des Betroffenen .....	129
4.4.3	Pflichten in Bezug auf das IKS .....	130
4.4.4	Vereinfachtes Sperren und Löschen per- sonenbezogener Daten – Auswirkungen auf das Berechtigungskonzept .....	131
4.4.5	Konkrete Anforderungen an das Berechtigungskonzept .....	133
4.4.6	Regelkonformität vs. Datenschutz .....	134
4.5	Allgemeine Anforderungen an ein Berechtigungskonzept .....	135
4.5.1	Identitätsprinzip .....	137
4.5.2	Minimalprinzip .....	137
4.5.3	Stellenprinzip .....	138
4.5.4	Belegprinzip der Buchhaltung .....	139
4.5.5	Belegprinzip der Berechtigungs- verwaltung .....	139
4.5.6	Funktionstrennungsprinzip .....	139
4.5.7	Genehmigungsprinzip .....	140
4.5.8	Standardprinzip .....	140
4.5.9	Schriftformprinzip .....	141
4.5.10	Kontrollprinzip .....	141
4.6	Fazit .....	142
<b>5</b>	<b>Berechtigungen in der Prozesssicht .....</b>	<b>143</b>
5.1	Prozessübersicht .....	143
5.2	Der Verkaufsprozess .....	145
5.3	Der Beschaffungsprozess .....	151
5.4	Unterstützungsprozesse .....	155
5.5	Maßgaben für die Funktionstrennung .....	158
5.6	Fazit .....	160

**TEIL II Werkzeuge und Berechtigungspflege im SAP-System****6 Technische Grundlagen der Berechtigungspflege ... 163**

6.1	Benutzer .....	163
6.2	Berechtigungen .....	173
6.2.1	Berechtigungsfelder und Berechtigungsobjekte .....	173
6.2.2	Berechtigungsprüfungen für ABAP- Programme .....	174
6.3	Rollen und Profile .....	176
6.3.1	Manuelle Profile und Berechtigungen .....	177
6.3.2	Rollenpflege .....	178
6.3.3	Massenpflege von Rollen .....	218
6.4	Transfer von Rollen .....	222
6.4.1	Rollentransport .....	223
6.4.2	Down-/Upload von Rollen .....	225
6.5	Benutzerabgleich .....	225
6.6	Vom Trace zur Rolle .....	227
6.7	Weitere Auswertungen von Berechtigungsprüfungen .....	234
6.7.1	Auswertung der Berechtigungsprüfung .....	234
6.7.2	Prüfung des Programms .....	236
6.8	Fazit .....	239

**7 Systemeinstellungen und Customizing ..... 241**

7.1	Pflege und Nutzung der Vorschläge für den Profilgenerator .....	242
7.1.1	Grundzustand und Pflege der Berechtigungsvorschlagswerte .....	244
7.1.2	Nutzen der Berechtigungs- vorschlagswerte .....	255
7.2	Traces .....	262
7.2.1	Vorgehen beim Berechtigungstrace .....	265
7.2.2	Vorgehen beim Systemtrace .....	269
7.2.3	Vorgehen beim Benutzertrace .....	270
7.3	Upgrade-Nacharbeiten von Berechtigungen .....	271
7.4	Parameter für Kennwortregeln .....	278
7.5	Menükonzept .....	284
7.6	Berechtigungsgruppen .....	290

7.6.1	Optionale Berechtigungsprüfungen auf Berechtigungsgruppen .....	292
7.6.2	Tabellenberechtigungen .....	297
7.6.3	Berechtigungsgruppen von Programmen ...	303
7.6.4	Berechtigungsgruppen als Organisationsebenen .....	304
7.7	Parameter- und Query-Transaktionen .....	305
7.7.1	Parametertransaktion zur Pflege von Tabellen über definierte Views .....	308
7.7.2	Parametertransaktion zur Ansicht von Tabellen .....	311
7.7.3	Querys in Transaktionen umsetzen .....	311
7.7.4	Zuordnung eines Programms zu einem Transaktionscode .....	314
7.8	Anhebung eines Berechtigungsfeldes zur Organisationsebene .....	315
7.8.1	Auswirkungsanalyse .....	315
7.8.2	Vorgehen zur Anhebung eines Feldes zur Organisationsebene .....	319
7.8.3	Anhebung des Verantwortungsbereichs zur Organisationsebene .....	321
7.9	Berechtigungsfelder und -objekte anlegen .....	323
7.9.1	Berechtigungsfelder anlegen .....	323
7.9.2	Berechtigungsobjekte anlegen .....	325
7.10	Weitere Transaktionen der Berechtigungsadministration .....	327
7.11	Fazit .....	329

**8 Rollenzuordnung über das Organisations-  
management ..... 331**

8.1	Grundkonzept des SAP-ERP-HCM- Organisationsmanagements .....	332
8.2	Fachliche Voraussetzungen .....	335
8.3	Technische Umsetzung .....	335
8.3.1	Voraussetzungen .....	335
8.3.2	Technische Grundlagen des SAP-ERP- HCM-Organisationsmanagements .....	336
8.3.3	Zuweisung von Rollen .....	336
8.3.4	Auswertungsweg .....	338
8.3.5	Benutzerstammabgleich .....	339

8.4	Konzeptionelle Besonderheit .....	339
8.5	Fazit .....	340

## **9 Zentrales Management von Benutzern und Berechtigungen ..... 341**

9.1	Grundlagen .....	342
9.1.1	Betriebswirtschaftlicher Hintergrund .....	342
9.1.2	User Lifecycle Management .....	345
9.1.3	SAP-Lösungen für die zentrale Verwaltung von Benutzern .....	348
9.2	Zentrale Benutzerverwaltung .....	348
9.2.1	Vorgehen zur Einrichtung einer ZBV .....	350
9.2.2	Integration mit dem Organisationsmanagement von SAP ERP HCM .....	356
9.2.3	Integration mit SAP Access Control .....	357
9.3	SAP Access Control User Access Management .....	358
9.4	SAP Identity Management .....	366
9.4.1	Funktionen .....	367
9.4.2	Technische Architektur .....	369
9.4.3	Komponenten und Architektur in SAP Identity Management 8.0 .....	373
9.4.4	Funktionsweise .....	374
9.4.5	Integration mit SAP Access Control .....	382
9.5	Compliant Identity Management .....	383
9.6	Fazit .....	385

## **10 Berechtigungen: Standards und Analyse ..... 387**

10.1	Standards und ihre Analyse .....	387
10.1.1	Rolle anstelle von Profil .....	388
10.1.2	Definition der Rolle über das Menü .....	389
10.1.3	Vorschlagsnutzung .....	391
10.1.4	Tabellenberechtigungen .....	391
10.1.5	Programmausführungsberechtigungen .....	392
10.1.6	Ableitung .....	393
10.1.7	Programmierung – Programmierrichtlinie .....	394
10.2	Kritische Transaktionen und Objekte .....	396
10.3	Allgemeine Auswertungen technischer Standards ....	398
10.3.1	Benutzerinformationssystem .....	398

10.3.2	Tabellengestützte Analyse von Berechtigungen .....	402
10.4	AGS Security Services .....	406
10.4.1	Secure Operations Standard und Secure Operations Map .....	408
10.4.2	Berechtigungs-Checks im SAP Early-Watch Alert und Security Optimization Service .....	409
10.4.3	Reporting über die Zuordnung kritischer Berechtigungen mithilfe der Configuration Validation .....	416
10.5	Fazit .....	418

## **11 SAP Access Control ..... 419**

11.1	Grundlagen .....	419
11.2	Access Risk Analysis .....	423
11.3	Business Role Management .....	429
11.4	User Access Management .....	431
11.5	Emergency Access Management .....	433
11.6	Fazit .....	436

## **12 User Management Engine ..... 437**

12.1	Überblick über die UME .....	438
12.1.1	UME-Funktionen .....	438
12.1.2	Architektur der UME .....	440
12.1.3	Oberfläche der UME .....	441
12.1.4	Konfiguration der UME .....	442
12.2	Berechtigungskonzept von SAP NetWeaver AS Java .....	446
12.2.1	UME-Rollen .....	446
12.2.2	UME-Aktionen .....	447
12.2.3	UME-Gruppe .....	448
12.2.4	Java-EE-Sicherheitsrollen .....	450
12.3	Benutzer- und Rollenadministration mit der UME ...	451
12.3.1	Voraussetzungen zur Benutzer- und Rollenadministration .....	451
12.3.2	Administration von Benutzern .....	452
12.3.3	Benutzertypen .....	453
12.3.4	Administration von UME-Rollen .....	454

12.3.5 Administration von UME-Gruppen ..... 456  
 12.3.6 Tracing und Logging ..... 456  
 12.4 Fazit ..... 458

**TEIL III Berechtigungen in spezifischen SAP-Lösungen**

**13 Berechtigungen in SAP ERP HCM ..... 461**

13.1 Grundlagen ..... 461  
 13.2 Besondere Anforderungen von SAP ERP HCM ..... 462  
 13.3 Berechtigungen und Rollen ..... 464  
     13.3.1 Berechtigungsrelevante Attribute in SAP ERP HCM ..... 464  
     13.3.2 Beispiel »Personalmaßnahme« ..... 466  
 13.4 Berechtigungshauptschalter ..... 470  
 13.5 Organisationsmanagement und indirekte Rollenzuordnung ..... 472  
 13.6 Strukturelle Berechtigungen ..... 474  
     13.6.1 Strukturelles Berechtigungsprofil ..... 475  
     13.6.2 Auswertungsweg ..... 476  
     13.6.3 Strukturelle Berechtigungen und Performance ..... 478  
     13.6.4 Anmerkung zu strukturellen Berechtigungen ..... 478  
 13.7 Kontextsensitive Berechtigungen ..... 479  
 13.8 Zeitabhängiges Sperren personenbezogener Daten ..... 481  
     13.8.1 Zeitabhängige Berechtigungsprüfung – Grundsätzliches ..... 481  
     13.8.2 Ablauf der zeitabhängigen Berechtigungsprüfung ..... 483  
     13.8.3 Einrichten der zeitabhängigen Berechtigungsprüfung ..... 483  
 13.9 Fazit ..... 486

**14 Berechtigungen in SAP CRM ..... 487**

14.1 Grundlagen ..... 488  
     14.1.1 Die SAP-CRM-Oberfläche: der CRM Web Client ..... 488

14.1.2 Erstellen von Benutzerrollen für den CRM Web Client ..... 496  
 14.2 Abhängigkeiten zwischen der Benutzerrolle und PFCG-Rollen ..... 498  
 14.3 Erstellen von PFCG-Rollen abhängig von Benutzerrollen ..... 500  
     14.3.1 Voraussetzungen für das Erstellen von PFCG-Rollen ..... 500  
     14.3.2 Erstellen von PFCG-Rollen ..... 503  
 14.4 Zuweisen von Benutzerrollen und PFCG-Rollen ..... 508  
 14.5 Beispiele für Berechtigungen in SAP CRM ..... 517  
     14.5.1 Berechtigen von Oberflächenkomponenten ..... 517  
     14.5.2 Berechtigen von Transaktionsstarter-Links ..... 526  
     14.5.3 Sonstige Berechtigungsmöglichkeiten für den CRM Web Client ..... 528  
     14.5.4 Berechtigen von Stammdaten ..... 530  
     14.5.5 Berechtigen von Geschäftsvorgängen ..... 533  
     14.5.6 Berechtigen von Attributgruppen ..... 543  
     14.5.7 Berechtigen von Marketingelementen ..... 544  
 14.6 Fehlersuche im CRM Web Client ..... 546  
 14.7 Access Control Engine ..... 549  
 14.8 Fazit ..... 563

**15 Berechtigungen in SAP SRM ..... 565**

15.1 Grundlagen ..... 565  
 15.2 Berechtigungsvergabe in SAP SRM ..... 568  
     15.2.1 Berechtigen der Oberflächenmenüs ..... 572  
     15.2.2 Berechtigen typischer Geschäftsvorgänge .. 574  
 15.3 Fazit ..... 588

**16 Berechtigungen in SAP BW ..... 589**

16.1 OLTP-Berechtigungen ..... 590  
 16.2 Analyseberechtigungen ..... 593  
     16.2.1 Grundlagen ..... 593  
     16.2.2 Schrankenprinzip ..... 595  
     16.2.3 Transaktion RSECADMIN ..... 596  
     16.2.4 Berechtigungspflege ..... 596

16.2.5	Massenpflege .....	600
16.2.6	Zuordnung zu Benutzern .....	600
16.2.7	Analyse und Berechtigungsprotokoll .....	604
16.2.8	Generierung .....	607
16.2.9	Berechtigungs migration .....	609
16.3	Modellierung von Berechtigungen in SAP BW .....	610
16.3.1	InfoProvider-basierte Modelle .....	611
16.3.2	Merkmalsbasierte Modelle .....	611
16.3.3	Gemischte Modelle .....	612
16.4	RBAC-Modell .....	612
16.5	Fazit .....	614

## **17 Berechtigungen in der SAP-BusinessObjects-Business-Intelligence-Plattform 4.x ..... 615**

17.1	Berechtigungskonzept .....	616
17.1.1	Benutzer und Benutzergruppen .....	617
17.1.2	Objekte, Ordner, Kategorien .....	620
17.1.3	Zugriffsberechtigungen .....	621
17.2	Interaktion mit SAP BW .....	624
17.2.1	System für Endbenutzer anschließen .....	625
17.2.2	Beispiel einer Anwendung: Query in Web Intelligence einbinden .....	626
17.3	Fazit .....	628

## **18 RFC-Sicherheit mittels Unified Connectivity ..... 631**

18.1	RFC-Sicherheit im Überblick .....	632
18.2	Das Konzept von Unified Connectivity .....	634
18.3	UCON einrichten und betreiben .....	637
18.4	Zusammenspiel von UCON und Berechtigungsprüfungen auf Funktionsbausteine .....	641
18.5	Fazit .....	648

## **19 Berechtigungen in SAP HANA ..... 649**

19.1	Anwendungsszenarien von SAP HANA .....	650
19.2	Architektur von SAP HANA .....	651
19.2.1	Sicherheitsarchitektur in SAP HANA .....	654
19.2.2	Objekte des Berechtigungswesens in SAP HANA .....	656

19.3	Benutzerverwaltung in SAP HANA .....	657
19.4	Berechtigungen in SAP HANA .....	660
19.4.1	Privilegien in SAP HANA .....	660
19.4.2	Rollen in SAP HANA .....	664
19.4.3	Beispiel für Berechtigungen in SAP HANA .....	665
19.5	Fazit .....	667

## **20 Berechtigungen in SAP S/4HANA ..... 669**

20.1	Überblick .....	669
20.2	Fiori-Anwendungsrollen anlegen .....	670
20.3	Kontinuität im Benutzermanagement .....	677
20.4	Fazit .....	677

## **21 SAP Business Suite: Prozesse und Einstellungen ... 679**

21.1	Grundlagen .....	680
21.1.1	Stamm- und Bewegungsdaten .....	680
21.1.2	Organisationsebenen .....	681
21.2	Berechtigungen im Finanzwesen .....	682
21.2.1	Organisatorische Differenzierungskriterien .....	683
21.2.2	Stammdaten .....	685
21.2.3	Buchungen .....	697
21.2.4	Zahllauf .....	702
21.3	Berechtigungen im Controlling .....	704
21.3.1	Organisatorische Differenzierungskriterien .....	705
21.3.2	Stammdatenpflege .....	706
21.3.3	Buchungen .....	715
21.3.4	Altes und neues Berechtigungskonzept im Controlling .....	718
21.4	Berechtigungen in der Logistik (allgemein) .....	718
21.4.1	Organisatorische Differenzierungskriterien .....	719
21.4.2	Materialstamm/Materialart .....	720
21.5	Berechtigungen im Einkauf .....	724
21.5.1	Stammdatenpflege .....	724
21.5.2	Beschaffungsabwicklung .....	724
21.6	Berechtigungen im Vertrieb .....	731

21.6.1	Stammdatenpflege .....	731
21.6.2	Verkaufsabwicklung .....	732
21.7	Berechtigungen in technischen Prozessen .....	735
21.7.1	Funktionstrennung in der Berechtigungsverwaltung .....	736
21.7.2	Funktionstrennung im Transportwesen .....	740
21.7.3	RFC-Berechtigungen .....	742
21.7.4	Debugging-Berechtigungen .....	743
21.7.5	Mandantenänderung .....	744
21.7.6	Änderungsprotokollierung .....	745
21.7.7	Batchberechtigungen .....	746
21.8	Vereinfachtes Sperren und Löschen personen- bezogener Daten in der SAP Business Suite .....	747
21.8.1	Konzept des vereinfachten Sperrens und Löschens personenbezogener Daten .....	748
21.8.2	Funktion in der SAP Business Suite .....	751
21.8.3	Berechtigungen für gesperrte Daten verwalten .....	754
21.9	Fazit .....	757

## **22 Konzepte und Vorgehen im Projekt ..... 759**

22.1	Berechtigungskonzept im Projekt .....	760
22.2	Vorgehensmodell .....	762
22.2.1	Logischer Ansatz .....	763
22.2.2	Implementierung .....	765
22.2.3	Redesign .....	766
22.2.4	Konkretes Vorgehen .....	767
22.3	SAP-Best-Practices-Template-Rollenkonzept .....	771
22.3.1	SAP Best Practices .....	771
22.3.2	SAP-Template-Rollen .....	772
22.3.3	Methodische Vorgehensweise des SAP- Best-Practices-Rollenkonzepts .....	774
22.3.4	Einsatz mit SAP Access Control .....	777
22.3.5	Template-Rollen für SAP HANA .....	778
22.4	Inhalte eines Berechtigungskonzepts .....	778
22.4.1	Einleitung und normativer Rahmen des Konzepts .....	779
22.4.2	Technischer Rahmen .....	781
22.4.3	Risikobetrachtung .....	781
22.4.4	Person – Benutzer – Berechtigung .....	782

22.4.5	Berechtigungsverwaltung .....	783
22.4.6	Organisatorische Differenzierung .....	784
22.4.7	Prozessdokumentation .....	784
22.4.8	Rollendokumentation .....	785
22.5	Schritte zum Berechtigungskonzept .....	785
22.5.1	Rahmenkonzept und Projektmitglieder .....	785
22.5.2	Rollenkonzept .....	786
22.5.3	Rollenimplementierung .....	791
22.5.4	Tests und Zuordnung zu Benutzern .....	791
22.6	Fazit .....	792

## **Anhang ..... 793**

A	Abkürzungsverzeichnis .....	795
B	Glossar .....	799
C	Literaturverzeichnis .....	815
D	Die Autoren .....	823
Index .....		827



# Index

OBI\_ALL 601, 603, 604  
OTCAACTVT 594, 596, 613  
OTCAIPROV 594, 596, 611, 613  
OTCAKYFNM 594  
OTCAVALID 594, 596, 597, 613

## A

ABAP 799  
ABAP Dictionary 799  
ABAP-Benutzertyp 454  
Abgabenordnung 799  
abgeleitete Rolle 578  
Ablauforganisation 71, 799  
    *betriebswirtschaftliches Berechtigungs-*  
    *konzept* 124  
    *ID Management* 346  
Ableitung von Rollen  
    *Abweichung* 393  
    *Manipulation* 393  
    *Referenzrolle* 212  
    *Standards* 393  
Ableitungskonzept 209, 315, 799  
Abstraktion 769  
AcceleratedSAP → ASAP  
Access Control Engine → ACE  
Access Control List 554, 560,  
    634, 799  
Access Control → SAP Access Control  
Access Risk Analysis → ARA  
ACE 488, 549, 799  
ACE Design Report 556  
ACE-Aktionsgruppe 799  
ACE-Aktivierungs-Tool 557  
ACE-Aktualisierungs-Tool 559  
ACE-Benutzergruppe 551, 799  
ACE-Laufzeitreport 558  
ACE-Recht 551, 799  
ACE-Regel 550, 551, 552, 799  
ACL 634  
Active Directory 799  
    *SAP ID Management* 366  
Actors from Object 552  
Actors from User 552  
Ad-hoc Query 307, 800  
Aggregationsberechtigung 597, 606

AGS Security Services 406  
AktG 800  
Aktengesetz → AktG  
Aktionsgruppe 551, 552  
Aktivität im Berechtigungskonzept 89  
Aktortyp 552, 800  
ALE 350  
alternative Hierarchien 711, 800  
    *Controlling* 97  
Ampelfarben 193  
Analyse von Berechtigungs-  
    prüfungen 234  
Analyseberechtigungen 589, 593, 595  
Analyse-Synthese-Konzept 80  
Analytics 567  
analytische Privilegien 662  
Angebot im Verkaufsprozess 146  
ANSI INCITS 51  
Anspruchsgruppen 39  
Anwendungen in entfernten  
    verbundenen Systemen 186  
Anwendungskatalog  
    *SAP S/4HANA* 672  
Anwendungsrollen  
    *SAP S/4HANA* 671  
Anzeigeattribute 594  
Application Link Enabling → ALE  
Application Programming Interface  
    (API) 441  
Applikationsprivilegien 661, 664  
ARA 422, 799  
Arbeitspaket 80, 553, 800  
Archivierung 593  
ARIS 38, 800  
ASAP 37, 800  
Attributgruppe 517, 543  
Audit 39, 256, 402, 682, 800  
Aufbauorganisation 71, 77, 79, 800  
    *betriebswirtschaftliches Berechtigungs-*  
    *konzept* 124  
    *SAP ERP* 92  
Aufgabe 39, 49, 77, 80, 86, 768, 800  
    *Berechtigungskonzept* 88  
    *Funktionstrennungskonflikt* 769  
Aufgabenanalyse 85, 767, 800  
    *Aufgabensynthese* 86, 768

Aufgabenanalyse (Forts.)  
   *Berechtigungskonzept* 49  
   *Objektanalyse* 85  
   *Stelle* 87  
   *Stellen- und Abteilungsbildung* 87  
   *Verrichtungsanalyse* 85  
 Auftragsart 106, 800  
 Auftragsbearbeiter 571  
 Auftrags erfassung im Verkaufsprozess 146  
 Auftragsposition 146  
 Auktion 566  
 Auswertung  
   *Profilzuordnung* 388  
   *über Status* 390  
 Auswertungsweg 476, 800  
   *Organisationsmanagement* 333  
 Authentifizierung in SAP HANA 660  
 Authority-Check 175, 236, 800

**B**

---

BANF 153, 728, 800  
 Barriereprinzip → Schrankenprinzip  
 Batchbenutzer 746  
 Batchberechtigungen 746  
 BDSG 126, 801  
 Beleg 575, 577, 801  
   *Bewegungsdaten* 681  
 Belegpositionsdaten 154  
 Belegprinzip 139  
 Benachrichtigungseinstellung im Workflow 363  
 Benachrichtigungs-E-Mail 445  
 Benutzer 163, 511, 617, 801  
   *Benutzerpflege* 165  
   *Dialogbenutzer* 164  
   *HCM-OM* 465  
   *Kommunikationsbenutzer* 165  
   *Mandant* 165  
   *Person* 166  
   *Protokollierungen von Systemzugriffen* 166  
   *Referenzbenutzer* 165  
   *SAP HANA* 656  
   *Servicebenutzer* 165  
   *Systembenutzer* 165  
 Benutzer synchronisieren (ZBV) 353  
 Benutzerabgleich 215, 225

Benutzeradministration 573  
 Benutzeranlage 167  
 Benutzerauthentifizierung 169  
 Benutzerdaten im Organisationsmanagement 344  
 Benutzerfehler 42  
 Benutzerfestwerte 169  
 Benutzergruppe 168, 513, 574, 587, 617, 618, 801  
 Benutzerinformationssystem 398  
 Benutzerkontext 553, 559  
 Benutzerkonto 342, 345  
 Benutzermenü 498, 505  
 Benutzerparameter 170, 515  
   *CRM\_UI\_PROFILE* 515  
   *ZBV* 349  
 Benutzerrolle 492, 493, 496, 498, 500, 503, 507, 510, 512, 514, 516, 518, 801  
   *Zuweisung* 508  
 Benutzerstammabgleich 339, 801  
 Benutzerstammsatz 437, 513  
   *Elemente* 165  
   *ID Management, Attribute* 349  
   *ZBV, zentrale und dezentrale Pflege* 353  
 Benutzertrace 264  
 Benutzertyp 165, 168, 453, 801  
 Benutzerverwalter 736  
 Benutzerverwaltung (Java) 438  
 Benutzer-Workflow 801  
 Benutzerzuordnung 601  
 Berechtigung 173, 801  
   *Debug/Replace* 413  
   *deklarative* 450  
   *ID Management, regelbasiertes* 344  
   *kontextsensitive* 479  
   *kritische* 44  
   *Nummer* 197  
   *programmatische* 451  
   *Standards* 387  
   *tabellengestützte Analyse* 402  
   *Upgrade* 259  
   *Vertragsverhältnis* 344  
   *verweigern* 622  
   *vorschlagsbasierte* 391  
 Berechtigungs-Check 409  
   *im EWA* 411  
   *im SOS* 413  
   *kundenspezifischer* 415

Berechtigungs-Check (Forts.)  
   *Struktur* 411  
 Berechtigungs differenzierung 79  
 Berechtigungserstellung 438  
 Berechtigungsfeld 173, 801  
   *ACTVT* 174, 613  
   *anlegen* 323  
   *LL\_TGT* 527  
   *LL\_TYPE* 527  
   *RESPAREA* 319, 709, 710, 810  
 Berechtigungsgruppe 290, 292, 303, 530, 801  
   *Debitor* 146  
   *Haushaltsmanagement* 292  
   *optionale Prüfung* 292  
   *organisatorisches Unterscheidungsmerkmal* 304  
   *Tabellenzugriff* 292  
 Berechtigungshauptschalter 801  
   *HCM* 470  
 Berechtigungskonzept 80, 446, 496, 526, 801  
   *Anforderungen* 135  
   *Aufgabenanalyse* 49  
   *Aufwand* 38  
   *Beschreibung* 51  
   *betriebswirtschaftliches* 37, 49  
   *Blueprints* 760  
   *Corporate Governance* 49  
   *Definition* 35, 47, 48  
   *Erweiterungsprojekt* 760  
   *Funktions trennung* 762  
   *heterogene Systemlandschaften* 760  
   *IKS* 760  
   *Inhalte* 49  
   *komponentenbezogenes* 37  
   *Kosten der Prävention* 49  
   *Kosteneinsparung* 761  
   *Partizipation* 39  
   *positives* 47  
   *Revision* 760  
   *SAP BusinessObjects* 616  
   *SAP-Einführung* 760  
   *Stammdaten* 680  
   *Standardisierung von Geschäftsprozessen* 760  
   *Standards* 760  
   *technisches* 48, 65  
   *Upgrade* 760  
   *Verfahrenssicht* 761

Berechtigungsmigration 609  
 Berechtigungsobjekt 173, 257, 396, 502, 567, 572, 575, 580, 801  
   */SAPCND/CM* 585  
   *B\_BUPA\_GRP* 530  
   *B\_BUPA\_RLT* 530, 585  
   *B\_BUPR\_BZT* 532  
   *BBP\_BUDGET* 586  
   *BBP\_CTR\_2* 582  
   *BBP\_FUNCT* 585, 586  
   *BBP\_PD\_AUC* 578  
   *BBP\_PD\_BID* 579  
   *BBP\_PD\_CNF* 579  
   *BBP\_PD\_CTR* 578, 582  
   *BBP\_PD\_INV* 579  
   *BBP\_PD\_PCO* 579  
   *BBP\_PD\_PO* 579  
   *BBP\_PD\_QUO* 579  
   *BBP\_PD\_SC* 579  
   *BBP\_PD\_VL* 579  
   *BBP\_SUS\_P2* 583  
   *BBP\_SUS\_PD* 583  
   *BBP\_VEND* 587  
   *C\_CABN* 543  
   *C\_KLAH\_BKL* 544  
   *C\_KLAH\_BKP* 543  
   *C\_LL\_TGT* 527  
   *C\_TCLA\_BKA* 544  
   *COM\_ASET* 584  
   *COM\_PRD* 532, 584  
   *COM\_PRD\_CT* 532  
   *CRM\_ACE\_MD* 560  
   *CRM\_ACT* 541  
   *CRM\_BPROLE* 530  
   *CRM\_CMP* 541  
   *CRM\_CO\_PU* 541  
   *CRM\_CO\_SA* 541  
   *CRM\_CO\_SE* 541  
   *CRM\_CO\_SL* 541  
   *CRM\_CON\_SE* 541  
   *CRM\_CPG* 544  
   *CRM\_CPGAGR* 544  
   *CRM\_CPGCTP* 544  
   *CRM\_CPGRES* 544  
   *CRM\_LEAD* 541  
   *CRM\_OPP* 541  
   *CRM\_ORD\_LP* 535, 540  
   *CRM\_ORD\_OE* 542  
   *CRM\_ORD\_OP* 534  
   *CRM\_ORD\_PR* 541

Berechtigungsobjekt (Forts.)  
 CRM\_SAO 541  
 CRM\_SEO 541  
 F\_REGU\_BUK 702  
 F\_REGU\_KOA 702  
 K\_CCA 711  
 K\_VRGNG 716  
 P\_PERNR 469  
 P\_TCODE 470  
 S\_BDC\_MONI 397  
 S\_CTS\_ADMI 741  
 S\_DEVELOP 392, 396, 397, 744  
 S\_LOG\_COM 397  
 S\_PROGNAM 176, 303  
 S\_PROGRAM 303  
 S\_RFC 176, 397, 641  
 S\_RS\_ALVL 590  
 S\_RS\_AUTH 591, 602  
 S\_RS\_HIST 591  
 S\_RS\_ICUBE 591  
 S\_RS\_ISNEW 590  
 S\_RS\_PLSE 590  
 S\_RS\_PLSQ 590  
 S\_RSEC 591  
 S\_SERVICE 176  
 S\_START 176  
 S\_TABU\_DIS 303, 305, 392, 396, 560, 641  
 S\_TABU\_NAM 299  
 S\_TCODE 389, 502, 506  
 Standardberechtigung 197  
 S\_USER\_AGR 739  
 S\_USER\_PRO 740  
 S\_USER\_SAS 739  
 SAP HANA 656  
 UIU\_COMP 500, 503, 506, 517, 521, 528  
 V\_VBAK\_AAT 733  
 V\_VBAK\_VKO 733

Berechtigungspflege  
 ALV-Sicht 190  
 Drag & Drop 203  
 generische Pflege 195  
 regelbasierte Pflege 255

Berechtigungsprofil  
 Nutzung ausschließen 388

Berechtigungsprotokoll 604, 605

Berechtigungsprüfung 595

Berechtigungsrelevanz 591, 594, 596

Berechtigungstrace 227, 263, 546, 643

Berechtigungsstyp 598

Berechtigungsvergabe  
 objektorientierte 620

Berechtigungsvorschlag 185

Berechtigungsvorschlagswert 177

Berechtigungsvorschlagswerte 645

Bereichsmenü 801

Bereichsstartseite 489, 493, 494, 495, 496, 505, 517, 520, 801

Beschaffungsprozess  
 Bestellung 151  
 Bewegungsart 154  
 Buchungskreis 152  
 Einkäufergruppe 153  
 Einkaufsorganisation 152  
 Freigabeverfahren 153  
 Lagerort 154  
 Lieferant 151  
 Rechnungsprüfung 151  
 Wareneingang 151

Bestellanforderung → BANF

Bestellung 726  
 Beschaffungsprozess 151  
 Bewegungsdaten 681

betrieblicher Datenschutz 126

Betriebsrat 74, 802  
 Datenschutz 125, 129

Betriebsverfassung 74, 802

betriebswirtschaftliches Berechtigungskonzept 760, 802  
 Ablauforganisation 124  
 Anforderungen 124  
 Aufbauorganisation 124  
 Benutzertypen 165  
 Berechtigungsverwaltung 783  
 Cross System Integration 762  
 Datenschutz 124  
 Datenschutzvorschriften 780  
 funktionale Differenzierung 761  
 Funktionstrennung 124  
 Genehmigung 780  
 Genehmigungsprinzip 783  
 Grundprinzipien 136  
 grüne Wiese 765  
 IKS 778  
 Implementierung 763  
 Inhalte 39, 778  
 institutioneller Rahmen 780

betriebswirtschaftliches Berechtigungskonzept (Forts.)  
 Konfiguration 782  
 kritische Aktion 124  
 Methode der Benutzerpflege 782  
 Methode der Berechtigungspflege 781  
 minimale Normen 780  
 Mitbestimmung 780  
 Organisationsabbildung 766  
 organisatorische Differenzierung 762, 784  
 Prozessabbildung 766  
 Rechnungslegungsvorschriften 780  
 Rechtsform 72  
 Redesign 763, 766  
 Risikobetrachtung 781  
 Schriftform 124  
 Schriftformprinzip 779  
 Standardprinzip 784  
 Stellenprinzip 783  
 Systemlandschaft 781  
 Teilkonzept 761  
 Vieraugenprinzip 784

Bewegungsart im Beschaffungsprozess 154

Bewegungsdaten 681

BI Launchpad 616

Bieter 570

BRF+ 361

BRM 422, 802

Browser 488

BSP 488, 573, 802

BSP-Applikation 488, 492, 501

BSP-Komponente 500

Buchhaltungsbeleg 154

Buchungen  
 Controlling 715  
 Finanzbuchhaltung 698

Buchungskreis 95, 103, 802  
 Beschaffungsprozess 152  
 Customizing 683  
 Verkaufsprozess 146

Bundesdatenschutzgesetz → BDSG

Business Planning and Simulation → BW-BPS

Business Role 492

Business Role Management → BRM

Business Server Pages → BSP

BusinessObjects-Server → SAP-BusinessObjects-BI-Plattform

Business-Rolle 770

BW-Berechtigungen 610

BW-Berechtigungsobjekte 592  
 S\_RS\_AUTH 591  
 S\_RSEC 591

BW-Berechtigungsprüfung 606

BW-BPS 590

## C

Catalog Content Management 566

Central Management Console → CMC

Checkpoint 548  
 CRM\_UIF\_NAV\_AUTH 548

Cloud Edition 669  
 SAP S/4HANA Cloud Edition 669

CMC 616

CobiT 116

Compliance 36, 40, 47, 802

Compliant Identity Management 384

Computing Center Management System (CCMS) 641

Configuration Tool 442

Configuration Validation 410, 416

Constrained RBAC 61, 63

Controlling 156

Core RBAC 53, 54

Corporate Governance 36, 45, 802  
 Definition 46  
 Managementaufgabe 46  
 Organisation 47

COSO-Rahmenkonzept 116

CRM Web Client 487, 488, 494, 496, 498, 500, 501, 511, 514, 802  
 Anmeldung 516

CRM\_UI\_PROFILE 515

CRM-Business-Objekt 488, 802

CRM-Navigationsleiste 489

Cross-Navigation 526

Crystal Reports 620

Customizing 487  
 Buchungskreis 683  
 Einkäufergruppe 719  
 Einkaufsorganisation 719  
 Faktura 734  
 Funktionsbereich 684  
 Gesellschaft 683  
 Kostenrechnungskreis 705  
 Lagerort 720

Customizing (Forts.)  
*Organisationsebene* 681  
*Profitcenter* 710  
*Sparte* 720  
*Verkäufergruppe* 719  
*Verkaufsorganisation* 719  
*Vertriebsauftragsart* 732  
*Vertriebsweg* 720  
*Werk* 719

## D

Dashboards → SAP BusinessObjects  
 Data Browser 298, 802  
*Zugriff ausschließen* 391  
 DataStore-Objekte → DSO  
 Datenquelle 443, 444, 452, 624  
 Datenschutz 802  
*betrieblicher* 126  
*Definition von personenbezogenen Daten* 127  
*elektronische Datenverarbeitung* 126  
 IKS 130  
*Logging* 134  
*Protokollierung der Programm-  
 nutzung* 134  
*Safe Harbor Privacy Principles* 126  
*Schweiz* 127  
*sensitive Daten* 127  
 Datenschutzgesetze der Länder 126,  
 802  
 Datenschutzleitfaden 116  
 Datenschutzrecht 124  
 Datenschutzrichtlinien 125  
 Datenselektion 595  
 Datenübermittlung (Datenschutz) 129  
 Datenverarbeitung (Datenschutz) 128  
 Debitor 802  
*Feldstatusgruppenpflege* 689  
*Funktionstrennung* 146  
*Stammdaten* 685  
*Stammdatum* 731  
*Verkaufsprozess* 145  
*Vieraugenprinzip* 146  
 Debitorenbuchhaltung 145  
 Debitorenpflege  
*buchhalterische Sicht* 145  
*logistische Sicht* 145  
*zentrale Sicht* 145

Debug/Replace 413  
 Debugging 803  
*Berechtigungen* 743  
 deduktiver Ansatz 111  
 Definition von personenbezogenen  
 Daten 127  
 deklarative Berechtigung 450  
 detektivische Kontrolle 119, 421, 427  
 Dialogbenutzer 164, 803  
*keine Profile* 388  
 Dienstleistungsbeschaffung 566  
 Differenzierungsschema 87  
 Directory Server Log 457  
 direkter Programmaufruf 304  
 Dokumente zu Bewegungsdaten 593  
 DSO 607  
 Dynamic Separation of Duty 61, 63

## E

EAM 202, 422, 433, 803  
 Eingabekontrolle 130  
 Einkauf, Berechtigungsprüfung für  
 Sachkonten 729  
 Einkäuferadministrator 570  
 Einkäufergruppe 107, 567, 577, 587,  
 803  
*Beschaffungsprozess* 153  
*Customizing* 719  
 Einkaufsorganisation 107, 567, 568,  
 572, 575, 577, 587, 803  
*Beschaffungsprozess* 152  
*Customizing* 719  
 Einkaufswagen 566, 569, 574, 576,  
 577, 579  
 Einlinienorganisation 77, 97  
 Elementarfunktion 768  
 E-Mail-Konto 342  
 Emergency Access Management  
 → EAM  
 End User Personalization → EUP  
 Endbenutzer  
*verbotene Transaktionen* 396  
 Enjoy-Transaktion 252, 726, 803  
 Ergebnisbereich 105  
 erweiterte Stammdatenprüfung im  
 Berechtigungshauptschalter 470  
 EUP 363  
 EWA 411  
 Excluding 597

Expertenmodus zur Profil-  
 generierung 198  
 externe Regeln 39  
 externer Service 500, 501, 502, 505,  
 507, 803

## F

F2-Hilfe 518, 522  
 Faktura 732, 803  
*Customizing* 734  
*Verkaufsprozess* 148  
 Fakturaart 734  
 FDA 765  
 Fehlersuche 549  
*im CRM Web Client* 546  
 Feldstatusgruppen 803  
 Feldstatusgruppenpflege  
*Debitor* 689  
*Kreditor* 689  
 Festwerte 169  
 Filterprinzip 595  
 Finanzbuchhaltung 95, 803  
 Finanzkreis 96  
 Finanzpositionenhierarchie 96  
 Finanzstellenhierarchie 96  
 Fiori 669  
 Fiori Launchpad 670  
 Firmenadresse (ZBV) 353  
 Fonds 96  
 Food and Drug Administration → FDA  
 Freigabestrategie 803  
*Beschaffung* 725  
*Beschaffungsprozess* 153  
*Finanzwesen* 699  
 Führungsaufgaben 36  
 Funktionsbereich 95, 104, 803  
*Berechtigungsgruppe* 684  
*Customizing* 684  
 Funktionstrennung 43, 139, 420,  
 736, 803  
*betriebswirtschaftliches Berechtigungs-  
 konzept* 124  
*Debitor* 146  
*Definition* 44, 123  
*dynamische* 61, 63  
*GoBS* 123  
*im Transportwesen* 740  
*Intersystemkonflikt* 150

Funktionstrennung (Forts.)  
*Intrasystemkonflikt* 150  
*Konfiguration* 770  
*Kosten* 45  
*Maßgaben* 158  
*Rollenzuweisung* 359  
*statische* 61, 63  
*unzureichende* 760  
*Zahllauf* 703

Funktionstrennungskonflikt 39, 44,  
 420, 767, 803  
*Identitätsprinzip* 166  
 Funktionstrennungsprinzip 139

## G

GDPdU 121  
 Genehmigungsprinzip 140, 803  
 Genehmigungsprozess 803  
*SAP ID Management* 368, 381  
 Genehmigungsverfahren 79  
 Genehmigungsworkflow 587  
 General Data Protection  
 Regulation 804  
 General IT Controls 130  
 Generierung 602, 607, 608  
 generische Pflege S\_TCODE 389  
 generischer Link 526  
 Geschäftsbereich 95, 103, 105, 804  
 Geschäftspartner 74, 145, 511, 517,  
 530, 567, 575, 584, 585, 804  
 Geschäftspartnerbeziehung 532  
 Geschäftspartnermanagement 93  
 Geschäftspartnerrolle 530  
 Geschäftsprozess 81, 679, 804  
 Geschäftsrollenhierarchie 804  
*SAP ID Management* 377  
 Geschäftsvorgang 511, 517, 533  
 Geschäftsvorgangsart 536, 804  
 Geschäftsvorgangstyp 541, 581, 804  
 Gesellschaft 95  
*Customizing* 683  
 Gesetz zur Kontrolle und Transparenz  
 in Unternehmen → KonTraG  
 GoB 120, 121, 139, 804  
 GoBD 122, 804  
 GoBS 121, 804  
 Grundsätze ordnungsgemäßer Buch-  
 führung → GoB

Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme → GoBS  
 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen 804  
 Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff 804  
 Gruppe mit direkten Links 489, 494, 804  
 Gültigkeitsbereich 598

## H

HANA → SAP HANA  
 Handelsgesetzbuch → HGB  
 Hashwert 505  
 HGB 120, 805  
 Hierarchische RBAC 57, 60  
 Hierarchieberechtigungen 596, 597  
 Hierarchiestruktur 598  
 Hosting 805  
 Hostingpartner 75, 805

## I

IAM 671  
 IC Web Client 487, 805  
 Identitätsprinzip 137, 167, 805  
 Identity and Access Management → IAM  
 Identity Management 137, 342, 366, 439  
 Identity Services 368  
 Identity Store 376  
 IKS 118, 805  
   *Berechtigungskonzept* 119  
   COSO 116  
   *Datenschutz* 130  
   *Definition* 118  
   *Grundlagen* 118  
   *Risikobeurteilung* 116  
 Implementierungsmethoden 765  
 Inbound-Plug 501, 503, 518, 805  
 indirekte Rollenzuordnung 472, 805  
   *Organisationsmanagement* 333

induktiver Ansatz 112, 763  
 InfoObjects 593  
 InfoProvider 611  
 Information und Kommunikation → IKS  
 Infotyp 465, 805  
   *0105 (Kommunikation)* 335  
   *IT0105 (Kommunikation)* 468  
   *Tabellen* 466  
 Initiator 361  
 In-Memory → SAP HANA  
 Innenauftrag 713, 805  
 institutioneller Organisationsbegriff 71  
   *Regelkonformität* 117  
 instrumenteller Organisationsbegriff 71, 76  
 Integration der Organisations-sichten 100  
 Integrierte Planung 593, 609  
 Interaktionskanäle 487  
 interne Regeln 72  
 Internes Kontrollsystem → IKS  
 Intervallberechtigungen 596  
 Intervallpflege S\_TCODE 389  
 IT Infrastructure Library → ITIL  
 IT-Grundschutzkatalog 805  
 ITIL 116  
 ITS 805

## J

J2EE-Sicherheitsrolle 805  
 Java 438  
 Java Connector → JCo  
 Java-Benutzertyp 454  
 Java-EE-Sicherheitsrolle 446, 450  
 JCo 444, 805  
 juristische Person 71

## K

Kalkulationsschema 732, 805  
 Kameralistik 120  
 Kategorie 621  
 Kennwort 167  
   *Gültigkeitsdauer* 281  
   *Missbrauch* 167  
 Kennworthistorie 281

Kennwortregel 167, 278, 445  
 Kennzahl 594  
 Kernprozess 144  
 Klassifikation 543  
 Kommunikationsbenutzer 444  
 kompensierende Kontrolle 421, 805  
 Komponentenfenster 501, 503, 518, 522  
 Komponentename 501, 518, 522  
 Komponenten-Plug 522  
 Kondition 585  
   *Verkauf* 731  
   *Verkaufsprozess* 146  
 Konditionen 806  
 Konditionsart 585  
 Konditionsfindung 146  
 Konditionspflege 731  
 Konfiguration der UME 442  
 Konnektor 806  
   *SAP ID Management* 368  
 Kontengruppe 146, 296, 686  
 Kontenplan 103, 806  
 Kontextlösung 479, 806  
   *Berechtigungs-hauptschalter* 470  
 kontextsensitive Berechtigungen 479, 806  
 Kontierungsobjekt 97, 806  
   *als Unterscheidungsmerkmal* 84  
   CO 156  
 KonTraG 121, 804, 806  
 Kontrollaktivitäten (IKS) 116  
 Kontrolle 806  
   *detektive* 421, 427  
   *kompensierende* 421  
   *präventive* 427  
 Kontrollprinzip 141  
 Kontrollumfeld im IKS 116  
 Kopfblock 495  
 Kosten und Leistungen 715  
 Kostenart 706, 806  
 Kostenrechnungskreis 104, 705, 806  
 Kostenstelle 97, 707, 806  
 Kostenstellenhierarchie 82, 92, 97, 98, 806  
 Kostenstellenrechnung 97  
 Kostenstellenstandardhierarchie 97, 105, 705  
 Kreditkontrolle 732  
 Kreditor 151, 806  
   *Feldstatusgruppenpflege* 689

Kreditor (Forts.)  
   *Stammdaten* 685  
   *Vieraugenprinzip* 152  
 Kreditorenbuchhaltung 151, 570  
 Kreditorenkonto 151  
 kriminelle Handlung 42  
 kritische Aktion 39, 44, 806  
   *betriebswirtschaftliches Berechtigungs-konzept* 124  
   *Datenschutz* 133  
   *Definition* 44, 124  
 kritische Berechtigung 44, 806  
   *Definition* 44  
   GoBS 123  
 kritische Berechtigungsobjekte 396  
 kritische Transaktionen 396  
 Kunde  
   *Geschäftspartner und Berechtigungen* 94  
   *Stammdatum* 731  
   *Verkaufsprozess* 145  
 kundeneigene Transaktion 807  
 Kunden-Exit 599  
 kurative Maßnahmen 43

## L

Lagerort 108, 807  
   *Beschaffungsprozess* 154  
   *Customizing* 720  
 Laufbahn  
   *Zugriffsrechte* 342  
 Layoutprofil 495  
 LDAP 438, 807  
 LDAP-Verzeichnis 438, 444  
 legale Normen 72, 114  
 Leistungserbringer 571  
 Leistungsverrechnung 156  
 Lieferant 570, 573, 574, 586, 587  
   *Beschaffungsprozess* 151  
   *Geschäftspartner und Berechtigungen* 94  
   *Stammdaten* 680  
 Lieferantenadministrator 571  
 Lieferantenbeziehung 565  
 Lieferantenqualifizierung 566  
 Lieferplan 732  
 Liefersperre im Verkaufsprozess 148  
 Lieferung im Verkaufsprozess 147

Lightweight Directory Access Protocol  
→ LDAP  
Linienorganisation 79, 807  
  *Organisationsmanagement* 332  
Linienvorgesetzter 84, 807  
Link, generischer → generischer Link  
Linkgruppe 493  
Log Viewer 457  
Logging 456, 807  
logischer Link 489, 493, 496, 503,  
  505, 517, 520, 807  
logisches System 807  
  ZBV 350  
Logondaten 168  
Löschen personenbezogener  
  Daten 747

## M

Manager 569  
Mandant 102, 807  
manueller Zahlungsausgang 700  
Marketingelement 517, 544  
Marketingmerkmal 543  
Massenpflege Berechtigungen 192,  
  203, 218, 600  
Maßnahmen  
  *kurative* 43  
  *präventive* 43  
Material 146, 807  
Materialart 721, 807  
Materialnummer 154  
Materialstamm 680, 720  
Matrixorganisation 807  
MaxAttention 407  
MDX 593  
Mehrlinienorganisation 77, 78  
Menü 505, 807  
Menüschafter im Customizing 287  
Metarollenhierarchie in SAP ID  
  Management 377  
Metarollenmodell 347  
Minimalprinzip 137  
  *GoBS* 123  
Missbrauch des Kennwortes 167  
Mitarbeiter 569  
  *Geschäftspartner und*  
  *Berechtigungen* 94  
Mitarbeitergruppe in HCM-OM 466  
Mitarbeiterkreis in HCM-OM 466

Mitbestimmung 74, 129  
Mobile Client 487  
Monitoring 807  
  *Datenschutz* 134  
Multidimensional Expressions → MDX  
Muster 596

## N

Navigationsleiste 489, 497  
Navigationsleistenprofil 492, 493,  
  495, 498, 518, 807  
Nebenbuchhaltung 145, 807  
neues Berechtigungskonzept im  
  Controlling 718  
Norm 808  
  *Vorschlagswerte* 259  
normativ 808  
normativer Rahmen  
  *Organisation* 118  
  *Regelkonformität* 117  
Notfallbenutzer 166, 396, 808  
Notfalluser-Management 63

## O

Oberflächenberechtigung 487, 517  
Objects by Filter 552  
Objektkontext 554, 559  
Objektprivilegien 661  
Objekttyp 465, 551  
OLAP 653, 808  
OLAP-Verbindungen 625  
OLTP 653, 808  
OneOrder-Objekt 808  
Online Analytical Processing → OLAP  
Online Transaction Processing  
  → OLTP  
On-Premise Edition  
  *SAP S/4HANA On-Premise*  
  *Edition* 669  
Operational Contract  
  Management 566  
operativer Einkäufer 569  
operativer Kontrakt 566  
optionale Prüfung 808  
Ordner 620  
Ordnerberechtigung 624  
Ordnerfreigabe 342

Organisation 808  
  *Ablauforganisation* 71  
  *Aufbauorganisation* 71, 77  
  *Begriff* 71  
  *Einlinienorganisation* 77  
  *institutioneller Begriff* 71, 72, 117  
  *instrumenteller Begriff* 71, 76  
  *Linienorganisation* 71, 77  
  *Organisationsformen* 71  
  *Projektorganisation* 71  
  *Prozessmodell* 72  
  *Rechenschaftspflichten* 76  
  *Rechtsform* 73  
  *Rechtsnormen* 73  
  *Stelle* 87  
  *zentrale Unterscheidungs-*  
  *merkmale* 109  
Organisationsebene 101, 808  
  *Auswertung der Nutzung* 767  
  *Berechtigungen* 101  
  *Customizing* 681  
  *Definition in Bezug auf*  
  *Berechtigungen* 102  
  *erstellen* 315  
  *kundeneigene* 101  
  *Stammdaten* 680  
  *Zuordnung* 682  
Organisationsebenenpflege 193  
Organisationseinheit 508  
  *HCM-OM* 465  
  *ID Management* 344  
Organisationsmanagement 332, 472,  
  705, 808  
  *Auswertungsweg* 333  
  *Benutzerdaten* 344  
  *indirekte Rollenzuordnung* 333  
  *Linienorganisation* 332  
  *Metarolle* 379  
  *Organisationseinheiten* 332  
  *Person* 332  
  *Planstelle* 332  
  *SAP ID Management und SAP Access*  
  *Control* 384  
  *SAP Identity Management* 367  
  *Stelle* 332  
  *ZBV* 356  
Organisationsmodell 508, 511, 512,  
  513, 514, 516, 535, 536, 537, 567,  
  568, 569, 575, 587

Organisationsschlüssel  
  in HCM-OM 466  
Organisationszweck 808  
  *Regelkonformität* 117  
organisatorische Differenzierung 808  
organisatorische Konzepte  
  in SAP ERP 93

## P

Paket 309  
Parameter 170  
  *auth/authorization\_trace* 265, 644  
  *auth/no\_check\_in\_some\_cases* 250  
  *auth/rfc\_authority\_check* 641  
  *login/password\_change\_waittime*  
  281  
  *login/password\_expiration\_time* 281  
  *login/password\_history\_size* 281  
  *login/accept\_sso2\_ticket* 279  
  *login/failed\_user\_auto\_unlock* 279  
  *login/fails\_to\_session\_end* 279  
  *login/fails\_to\_user\_lock* 280  
  *login/min\_password\_diff* 280  
  *login/min\_password\_digits* 280  
  *login/min\_password\_letters* 280  
  *login/min\_password\_lng* 280  
  *login/min\_password\_lowercase* 280  
  *login/min\_password\_specials* 281  
  *login/min\_password\_uppercase* 281  
  *login/password\_downwards\_*  
  *compatibility* 281  
  *login/password\_max\_idle\_initial* 281  
  *login/password\_max\_idle\_*  
  *productive* 281  
  *ucon/rfc/active* 639  
Parameter Customizing  
  *ADD\_COMPOSITE\_ROLES* 223  
  *ALL\_USER\_MENU\_OFF* 288  
  *CLIENT\_SET\_FOR\_ROLES* 224  
  *COLL\_READ\_LEVEL\_1* 288  
  *CONDENSE\_MENU* 288  
  *CONDENSE\_MENU\_PFCG* 288  
  *CUSTOMER\_MENU\_OFF* 288  
  *DELETE\_DOUBLE\_TCODES* 288  
  *GEN\_PSW\_MAX\_DIGITS* 282  
  *GEN\_PSW\_MAX\_LENGTH* 282  
  *GEN\_PSW\_MAX\_LETTERS* 282  
  *GEN\_PSW\_MAX\_SPECIALS* 282

- Parameter Customizing (Forts.)
  - PERSDAT\_TRANSPORT 223
  - PROFILE\_TRANSPORT 223
  - SAP\_MENU\_OFF 288
  - SGL\_ROLES\_TRANSPORT 223
  - US\_ASGM\_TRANSPORT 223
- Parameter Sicherheitsrichtlinie
  - CHECK\_PASSWORD\_BLACKLIST 284
  - DISABLE\_TICKET\_LOGON 283
  - MAX\_FAILED\_PASSWORD\_LOGON\_ATTEMPTS 283
  - MIN\_PASSWORD\_DIFFERENCE 283
  - MIN\_PASSWORD\_DIGITS 283
  - MIN\_PASSWORD\_LENGTH 283
  - MIN\_PASSWORD\_LETTERS 283
  - PASSWORD\_CHANGE\_INTERVAL 284
  - SERVER\_LOGON\_PRIVILEGE 284
- Parametertransaktionen 308, 808
- Partner Channel Management 550
- Partnerfunktion 533, 808
- Path 364
- People-Centric UI 487
- Permission 446, 447, 808
- Persistenzmanager 441, 809
- Person 809
  - Geschäftspartner und Berechtigungen 94
  - ID Management 344
  - Organisationsmanagement 332, 465
- Personalbereich in HCM-OM 466
- Personalisierung 492, 587
- Personalnummer, Berechtigungs-  
hauptschalter 470
- Personalrat 74
  - Datenschutz 125
- personenbezogene Daten 747
- PFCG-Rolle 179, 449, 452, 487, 493, 495, 496, 498, 500, 503, 505, 512, 514, 550, 567, 568, 574
  - Ableitungskonzept 209
  - Benutzerabgleich 215
  - Expertenmodus zur Profilgenerierung 198
  - Zuweisung 508
- Plan-Driven Procurement → planungs-  
gesteuerte Beschaffung
- Planstelle 508, 510, 512, 513, 575, 809
  - HCM-OM 465
  - ID Management 344
  - Organisationsmanagement 332
- planungsgesteuerte Beschaffung 566, 570
- Planungsstatus in HCM-OM 466
- Planvariante in HCM-OM 465
- Portalberechtigung 567, 568
- Portalintegration 488
- Portalrolle 437, 573, 588, 809
- Position
  - Zugriffsrechte 342
- präventive Kontrolle 119, 427, 809
- präventive Maßnahmen 43, 809
- Primärkosten 156, 809
- Primärkostenart 706
- Prinzipale 619, 623
- Privilegien in SAP HANA 656, 660
- Privilegientypen
  - Repository-Privilegien 661
- Produkt 530, 532
- Profil 177, 388, 514
  - ZBV 349
- Profilanalyse 388
- Profilart 495
- Profilgenerator 388, 809
- Profilname 189
- Profilpflege 388
- Profilverwalter 736
- Profilzuordnung 172, 388
- Profit-Center 105, 710, 809
- Profit-Center-Hierarchie 97, 705
- Programm
  - Berechtigungsprüfung 394
  - kundeneigenes 394
- programmatische Berechtigung 451
- programmatische Berechtigungs-  
prüfung 447
- Programmausführungs-  
berechtigung 392
- Programmierrichtlinie 394
- Projektorganisation 77, 79
- Projektstrukturplan 99
- Protokollierung 809
- Protokollierungen von System-  
zugriffen eines Benutzers 166
- Prozess 81, 809
- Prozesskontrolle 43, 809

- Prozessmodell 38
  - Prozessorganisation 77
  - Prüfkennzeichen 250
  - Prüfung der rechnerischen
    - Richtigkeit 151
  - Prüfung der sachlichen
    - Richtigkeit 151
- 
- Q**
- 
- Query 306, 311, 391, 594, 809
  - Questionnaire im SOS 414
  - QuickView 391
- 
- R**
- 
- Radierverbot 809
    - Debugging 44
  - RBAC 51
    - Begriffe 52, 55
    - Component 52
    - Constrained 61, 63
    - Core 53, 54
    - Hierarchical 57, 60
    - Kernelemente 52
    - Objects 52
    - Operations 52
    - Permission 54
    - Permissions 53
    - Restriktionen 64
    - Roles 53
    - Session 53
    - Session\_Roles 53
    - Subordinate Role 58, 60
    - Superior Role 58
    - Übertragung auf BW 612
    - Übertragung auf SAP ERP 54
    - User 53
    - User\_Sessions 53
  - RBAC-Standard Rollenkonzept 51
  - rechnerische Richtigkeit 809
  - Rechnungslegungsgrundsätze 73
  - Rechnungsprüfung 730
    - Beschaffungsprozess 151
  - Rechnungssteller 571
  - Rechnungsnormen 73
  - Rechtsquellen für das externes  
Rechnungswesen 120
  - redundanzfreies Menü 285
  - Referenzbeleg 732
  - Referenzbenutzer 172, 809
    - ZBV 349
  - Referenzrolle 212, 809
  - Regel
    - externe 39
    - interne 39
  - Regelkonformität 41, 114, 810
    - Branche 118
    - Compliance 40
    - Datenschutzleitfaden 116
    - Gebot 115
    - ID Management 346
    - internationale Normen 114
    - IT-Grundschatzkatalog 116
    - Kontrolle 40
    - normativer Rahmen 117
    - Organisation 40
    - Rechtsform 115, 117
    - rechtsgleiche Normen 115
    - Schaden 41
    - Sicherheitsleitfäden von SAP 116
    - soziale Normen 114
    - Stakeholder-Normen 114
    - Standards 114
    - Verbot 115
    - Vertrag 118
    - vertragliche Normen 114
    - Vorschlagswerte 260
    - Ziel 47
  - Regelwerk 419, 423
  - Regelwerk der Organisation 39
  - Remote Function Call → RFC
  - Remote Function Module → RFM
  - Remote Services für die Sicherheit  
407
  - remotefähige Funktionsbausteine 631
  - Report
    - CRMD\_UI\_ROLE\_ASSIGN 513, 514
    - CRMD\_UI\_ROLE\_PREPARE 504, 517
    - CRMD\_UI\_ROLE\_REPARE 507
    - PFCG\_ORGFIELD\_CREATE (Profilgenerator:Neues Org.-Ebenen-Feld anlegen) 319
    - PFCG\_ORGFIELD\_ROLES 321
    - PFCG\_ORGFIELD\_UPGRADE (Anpassung nach Upgrade für neue Org.-Ebenen ausführen) 275

- Report (Forts.)  
*PFCG\_TIME\_DEPENDENCY* (Massenabgleich) 339  
*RHAUTUPD\_NEW* (Abgleich Benutzerstamm) 339  
*RSPARAM* (Anzeige der SAP-Profilparameter) 278  
 Report Painter 810  
 Report Writer 810  
 Reporting-Berechtigungen 609  
 Repository-Privilegien 661, 663  
 Requester 577  
 RFC 165, 631, 742, 810  
   Berechtigungen 742  
   Trusted 742  
   Untrusted 742  
   ZBV 351  
 RFC-Destinationen 632  
 RFC-Statistiksätze 643  
 RFC-Verbindungen 632  
 RFM 631  
 Risiko  
   aktivitätsbezogenes 41  
   Definition 41  
   Definition für Berechtigungen 43  
   Funktionstrennung 43  
   Grenzen der Erfassung 44  
   Kosten der Erfassung 45  
   Organisationsziel 41  
   prozessuales 41  
   strategisches 41  
 Risikomanagement 42  
 Role Based Access Control  
   RBAC 52  
 Role Based Access Control → RBAC  
 Rolle 49, 176, 388, 810  
   abgeleitete 393  
   ableiten 209  
   Ableitungskonzept 209  
   Anwendungen in entfernten verbundenen Systemen 186  
   Automatisierung 227  
   Benutzerabgleich 215  
   Berechtigungen ermitteln 227  
   Berechtigungen, Ampel 193  
   Berechtigungstrace 227  
   betriebswirtschaftliche 50  
   Definition durch Transaktionen 389  
   Definiton 178  
   Download 225

- Rolle (Forts.)  
   Einzelrolle 60, 181  
   Expertenmodus zur Profilgenerierung 198  
   generische Pflege 195  
   HCM-OM 465  
   Hierarchie 59  
   Menü 184, 185  
   Menü aus anderer Rolle 185  
   Namenskonvention 179  
   Organisationsebenen 193  
   Pflegestatus von Berechtigungen 196, 208  
   Profilgenerator 178  
   Profilname 189  
   Referenzrolle 212  
   Sammelrolle 60, 181, 216  
   SAP HANA 656, 664  
   stellenbasierte Vergabe 90  
   Systemtrace 232  
   technische 50  
   Trace 227  
   Trace auswerten 232  
   Transport 223  
   Upgrade 272  
   Upload 225  
   Web-Dynpro-Anwendungen 186  
   Web-Dynpro-Konfigurationen 186  
   ZBV 349  
   Zuordnung 170  
 Rollenadministrator 736  
 Rollenhierarchie  
   allgemeine 59, 60  
   limitierte 59, 60  
 Rollenimport 617  
 Rollenkonfigurationsschlüssel 495, 810  
 Rollenkonzept im RBAC 51  
 Rollenmanager 810  
 Rollenmenü 505  
 Rollenpflege 389  
 Rollentransport 223  
 Route Mapping 364  
 RSECADMIN (Analyseberechtigungen) 596  
 RSECAUTH (Analyseberechtigungen pflegen) 596

## S

- SAAB 548  
 SACF 633  
 Sachkontenstammsatz 686  
 Sachkonto  
   Stammdaten 680, 685  
 sachliche Richtigkeit 810  
 Safe Harbor Privacy Principles 810  
 Sammelrolle 216, 516  
   Kontext Organisation 90  
 Sammelrollen 620  
 SAP Access Control 362, 419, 762, 785, 810  
   Access Risk Analysis (ARA) 422, 799  
   Benutzerverwaltung 358  
   Benutzer-Workflow 431  
   BRF+ 360, 361, 362  
   Business Process 423  
   Business Role Management (BRM) 422, 429, 802  
   Detour 364  
   EmergencyAccessManagement (EAM) 422, 433, 803  
   End User Personalization 361, 363  
   Funktion 424  
   Funktionstrennungskonflikt 423, 424  
   HANA 659  
   ID Management und Organisationsmanagement 384  
   Initiator 361  
   kompensierende Kontrolle 424, 426  
   Kontrollleur 434  
   kritische Aktion 423, 424  
   kritische Berechtigungen 423, 424  
   MSMP-Workflow 360  
   Path 361, 364  
   Regeln 426  
   Regelwerk 419, 423  
   Risiko 423  
   Route Mapping 361, 364  
   Routing 433  
   SAP ID Management 382  
   Segregation of Duties (SoD) 423  
   Stage 361, 432  
   Standardregelwerk 426  
   Superuser-ID 434  
   User Access Management (UAM) 348, 357, 422, 431, 813
- SAP Access Control (Forts.)  
   Verantwortlicher 435  
   Vorschlagswerte 260  
   Workflow 359  
   ZBV 357  
 SAP Active Global Support 407  
 SAP Business Suite 487  
 SAP Business Suite on SAP HANA 650  
 SAP BusinessObjects 615, 626  
   BI-Plattform 615  
   CMC 616  
   Dashboards 620  
   Web Intelligence 620, 626  
 SAP BW 566, 589  
 SAP CRM 487  
 SAP Customer Relationship Management → SAP CRM  
 SAP DB Control Center 652  
 SAP EarlyWatch Alert 103  
 SAP EarlyWatch Alert → EWA  
 SAP End-to-End Solution Operations  
   Standard for Security → Secure Operations Standard  
 SAP Enterprise Portal 437, 441, 567, 568, 573, 574, 588  
 SAP Enterprise Support 407  
 SAP ERP 566  
 SAP Gateway 633  
   reginfo 634  
   secinfo 634  
 SAP GUI 487, 488, 502, 511, 516  
 SAP HANA 649  
   analytische Privilegien 661, 662, 666  
   Anwendungsszenarien 650  
   Applikationsprivilegien 661, 664  
   Architektur 651  
   Audit Logging 655  
   Authentifizierung 654, 660  
   Benutzer 656  
   Benutzertypen 657  
   Benutzerverwaltung 658  
   DBMS 658  
   HALM 654  
   In-Memory 811  
   In-Memory-Technologie 652  
   Katalogobjekt 653  
   Objekt 656  
   Objekte Berechtigungswesen 656  
   Objektprivilegien 661  
   Owner-Konzept 653



SAP HANA (Forts.)  
*Passwort-Sicherheitsrichtlinien* 660  
*Privileg* 656  
*Privilegien* 660  
*Repository* 653  
*Repository-Objekte* 653  
*Repository-Objekte transportieren* 654  
*Repository-Privilegien* 661, 663  
*Restricted User* 657  
*Rolle* 656, 664  
*Rollenhierarchie* 664  
*SAP Identity Management* 659  
*Sicherheitsarchitektur* 654, 655  
*SSL-Verschlüsselung* 655  
*Standard User* 657  
*SYSTEM-Benutzer* 658  
*Systemprivilegien* 661  
*Transaktion SU01* 658  
SAP HANA Appliance 651  
SAP HANA Cockpit 652  
SAP HANA Datenbank 651, 811  
SAP HANA Live 650  
SAP HANA Persistenz 650, 811  
SAP HANA Realtime-Analysen 650, 811  
SAP HANA Security Guide 660  
SAP HANA Studio 651, 654  
SAP HANA View 650  
SAP HANA XS 652  
SAP Identity Management 348, 438  
*Genehmigungsprozess* 381  
*HANA-Anbindung* 659  
*Organisationsmanagement* 384  
*SAP Access Control* 382  
*Self-Services* 381  
*Vertretungsregelung* 381  
SAP Information Lifecycle Management (ILM) 750  
SAP NetWeaver Application Server  
*SAP NetWeaver AS ABAP* 567, 574  
SAP NetWeaver Application Server  
ABAP → SAP NetWeaver AS ABAP  
SAP NetWeaver Application Server  
Java → SAP NetWeaver AS Java  
SAP NetWeaver AS ABAP 437  
SAP NetWeaver AS Java 437  
SAP S/4HANA 669  
SAP Security Baseline 416  
SAP Solution Manager 408, 785

SAP SRM 437, 565  
*Berechtigungsvergabe* 568  
*Oberfläche* 567  
SAP Supplier Relationship Management → SAP SRM  
SAP\_ALL 75, 602  
SAP\_CRM\_UIU\_FRAMEWORK 514, 525  
SAP\_J2EE\_ADMIN 452  
SAP\_NEW 277  
SAP-Benutzerkonto  
*ID Management* 342  
SAP-Best-Practices-Ansatz 771  
SAP-Best-Practices-Template  
*Rollen* 772  
*Rollenkatalog* 773  
*Rollenkonzept* 771  
SAP-Einführung  
*Teilprojekt Berechtigungen* 38  
SAP-Fiori-Applikationen 669  
SAPJSF 444  
SapWorkDir-Verzeichnis 504  
Sarbanes-Oxley Act → SOX  
Satzung 73  
schaltbaren Berechtigungsprüfungs-szenarien 633  
Schrankenprinzip 595  
Schriftformprinzip 35, 141, 811  
Schutzbedarfsanalyse 764  
Secure Network Communication 633  
Secure Network Communications  
→ SNC  
Secure Operations Map 408, 409  
Secure Operations Standard 408  
Security Audit Log 456  
Security Log 456  
Security Optimization Service → SOS  
Segregation of Duties → Funktions-trennung  
Sekundärkosten 156, 811  
Sekundärkostenart 706  
Self-Service 566, 569, 570, 574, 577  
*SAP ID Management* 381  
Self-Service Procurement 566  
sensitive Daten 811  
*Datenschutz* 127  
Service Procurement 566  
Service, externer → externer Service  
Session\_Roles in RBAC 53  
Sicherheitskonzept 443, 445

Single Sign-on → SSO  
SNC 169, 633  
SOS 409  
*Questionnaire* 414  
*Whitelist* 414  
SOX 811  
soziale Normen  
*Definition* 117  
*Regelkonformität* 114  
Sparte 108, 811  
*Customizing* 720  
*Verkaufsprozess* 146  
Sperrungen personenbezogener  
Daten 747  
Spezialmerkmale 594, 596  
SQL-Trace (Datenschutz) 134  
SRM-Geschäftsprozesse 568  
SRM-Geschäftsszenarien 565, 573  
SRM-Geschäftsvorgänge 574  
SRM-Server 574  
SRM-Standardrolle 565  
SSO 169, 279, 440, 626, 811  
SSO-Ticket 279  
staatlicher Zugriff auf Daten 115  
Stage 362  
Staging 593  
Stakeholder 76  
Stakeholder-Ansatz 39, 812  
Stakeholder-Normen  
*Definition* 117  
*Regelkonformität* 114  
Stammdaten 511, 530, 575, 584, 680  
*Berechtigungskonzept* 680  
*Controlling* 704  
Stammdatenprüfung im Berechtigungs-hauptschalter 470  
Standardberechtigung im S\_TCODE 197  
Standardprinzip 140  
Standardrolle 525, 568, 571, 574  
Standards 812  
*Berechtigungen* 387  
Standards und internationale  
Normen 115  
Standardtransaktionen  
*Vorschlagswerte* 259  
Startberechtigung  
*externer Service* 176  
*RFC-Funktionsbaustein* 176  
*Service mit Objektkatalogeintrag* 176

Startberechtigung (Forts.)  
*Web-Dynpro-Anwendung* 176  
*Web-Dynpro-Konfiguration* 176  
Startberechtigungsprüfung 175  
Startmenü 169  
Static Separation of Duty 61, 63  
Status  
*Berechtigungsobjekt* 257  
*gepflegt* 197, 209, 258  
*manuell* 209, 257  
*Standard* 196, 208, 258  
*verändert* 257  
Stelle 77, 87, 768, 812  
*HCM-OM* 465  
*ID Management* 344  
*Organisationsmanagement* 332  
Stellenprinzip 138  
Strategic Sourcing 566  
strategische Bezugsquellenfindung 566  
strategischer Einkäufer 569  
strukturelle Berechtigungen 812  
*Berechtigungshauptschalter* 470  
*Organisationsmanagement* 472  
*organisatorische Differenzierung* 474  
*Risikoanalyse* 478  
*SAP Access Control* 479  
strukturelle Profile 349, 475, 812  
Subordinate Role 58  
Subtyp 465  
Suchseiten 491, 495  
Superior Role 58  
Superobjekttypen 551  
Supplier Qualification 566  
Supplier Self-Service 570, 574, 575, 586  
Switchable Authorization Check Framework 633  
Systembenutzer 444, 812  
Systemprivilegien 661  
Systemtrace 232, 265, 268, 546, 642  
Systemzugriff 343

**T**

Tabelle  
*AGR\_1251* 394  
*AGR\_DEFINE* 394  
*Berechtigungsadministration* 403

## Tabelle (Forts.)

CRMC\_UI\_COMP\_IP 521, 524  
 SSM\_CUST 287  
 TSTC 395  
 USOBT 500  
 USOBT\_C 500  
 USOBX 263  
 USOBX\_C 500  
 USR10 388  
 UST04 389  
 Tabellenberechtigung 391  
 Tabellenzugriffsrecht 392  
 technisches Berechtigungskonzept 812  
 technisches Profil 495  
 Teilaufgabe 39, 80, 86, 768, 812  
   *Berechtigungskonzept* 88  
 Tochtersystem (ZBV) 351  
 Toleranzzeitraum, Berechtigungs-  
 hauptschalter 470  
 Trace 227, 262, 456, 812  
   *Benutzertrace* 264  
   *Berechtigustrace* 263  
   *Systemtrace* 264  
 Trace-Datei 457  
 Transaktion 812  
   *Berechtigungspflege* 328  
   CRMC\_UI\_NBLINKS 493, 520  
   CRMC\_UI\_PROFILE 496, 519  
   DBCO 658  
   *Endbenutzer* 396  
   *entfernen* 258  
   *F-28 (Zahlungseingang buchen)* 700  
   *F-53 (Zahlungsausgang buchen)* 700  
   *FB60 (Kreditorenrechnung erfassen)*  
   699  
   *FB70 (Debitorenrechnung erfassen)*  
   699  
   *HR:OOAC (Berechtigungs-  
   hauptschalter)* 470  
   KA01 (*Kostenart anlegen*) 706  
   KA02 (*Kostenart ändern*) 706  
   KA06 (*Kostenart sekundär: anlegen*)  
   706  
   KCHN5N (*Standardhierarchie ändern*)  
   712  
   KE51 (*Profit-Center anlegen*) 712  
   KE52 (*Profit-Center ändern*) 712  
   *Kreditorenpflege* 294  
   *kritische* 396

## Transaktion (Forts.)

KS01 (*Kostenstelle anlegen*) 707  
 KS02 (*Kostenstelle ändern*) 707  
 KSH1 (*Kostenstellengruppe anlegen*)  
 708  
 LISTCUBE 593  
 ME21N (*Bestellung anlegen*) 726  
 ME22N (*Bestellung ändern*) 726  
 ME23N (*Bestellung anzeigen*) 252,  
 726  
 MIGO (*Warenbewegung*) 729  
 MIR7 (*Wareneingang vorerfassen*)  
 730  
 MIRO (*Eingangsrechnung erfassen*)  
 698, 730  
 OKEON (*Kostenstellenstandard-  
 hierarchie ändern*) 707  
 OKKP (*Sicht Komponenten aktivieren/  
 Steuerungskennzeichen ändern*)  
 711  
 PA30 (*Personalstammdaten pflegen*)  
 467  
 PA40 (*Personalmaßnahme*) 336  
 PA40 (*Pflege über Personal-  
 maßnahmen*) 467  
 PFCG (*Pflege von Rollen*) 179, 400  
 PFCGMASVAL 218  
 PFUD 226  
 PFUD (*Abgleich Benutzerstamm*)  
 339  
 PPOCA\_BBP 576  
 PPOMA\_BBP 567, 568, 576  
 PPOMA\_CRM 508  
 PPOME (*Organisation und Besetzung  
 ändern*) 336  
 RSECADMIN (*Analyseberechtigungen*)  
 596  
 RSECAUTH (*Analyseberechtigungen  
 pflegen*) 596  
 RSU01 (*Benutzerzuordnung BW*)  
 601  
 RSUDO 604  
 RZ10 (*Pflege der Profilparameter*)  
 278  
 RZ11 (*Pflege der Profilparameter*)  
 264  
 RZ11 (*Profilparameter*) 745  
 S\_ALR\_87101219 392  
 SA38 303

## Transaktion (Forts.)

SA38 (*Programmausführung*) 319,  
 392, 396, 504, 513  
 SAAB 548  
 SCC4 (*Mandantenverwaltung*) 744  
 SE13 (*Speicher-Param. für Tabellen  
 pflegen*) 745  
 SE16 (*Data Browser*) 298, 392, 395,  
 521  
 SE16N (*Allgemeine Tabellenanzeige*)  
 306  
 SE17 (*Allgemeine Tabellenanzeige*)  
 306  
 SE38 (*ABAP Editor*) 395  
 SE54 (*Generierung Tabellensicht*)  
 302  
 SE80 (*Object Navigator*) 236  
 SE93 (*Transaktionspflege*) 308  
 SM12 (*Sperren anzeigen und löschen*)  
 398  
 SM13 (*Verbuchungssätze adminis-  
 trieren*) 398  
 SM30 (*Aufruf View-Pflege*) 306  
 SM35 (*Batch-Input-Monitoring*) 397  
 ST01 546, 549  
 START\_REPORT 303  
 SU01 658  
 SU01 (*Benutzerpflege*) 167, 349,  
 511, 514, 573  
 SU02 (*Profile*) 388  
 SU20 (*Pflege der Berechtigungs-  
 felder*) 323  
 SU21 (*Pflege der Berechtigungs-  
 objekte*) 325, 544, 580  
 SU22 (*Pflege der Zuordnung von  
 Berechtigungsobjekten*) 502  
 SU24 (*Berechtigungsobjektprüfung  
 unter Transaktion*) 502, 507  
 SU24 (*Pflege der Berechtigungsvor-  
 schlagswerte*) 500  
 SU25 (*Upgrade-Tool für den Profil-  
 generator*) 259, 272  
 SU53 (*Auswertung der Berechtigungs-  
 prüfung*) 234, 547  
 SUB% 303  
 SUIM (*Benutzerinformationssystem*)  
 398, 547  
 VF01 (*Anlegen Faktura*) 698  
 VF01 (*Faktura anlegen*) 735  
 VF02 (*Ändern Faktura*) 698

## Transaktion (Forts.)

VF02 (*Faktura ändern*) 735  
 VK31 (*Konditionen anlegen*) 731  
 VK32 (*Konditionen ändern*) 731  
 VK33 (*Konditionen anzeigen*) 731  
 VL01N (*Lieferung anlegen*) 734  
 VL02N (*Lieferung ändern*) 734  
 Transaktionscode 812  
 Transaktionsstarter 526  
 Transportauftrag Vorschlagswerte  
 253  
 True and Fair View 48, 704, 779, 812  
 Trusted RFC 742

## U

UAM 348, 357, 422, 431, 813  
 Übersichtsseite 491, 495  
 Überwachung im IKS 116  
 UCON 632, 634  
   *Auswertungsphase* 636, 641  
   *Communication Assembly (CA)* 635  
   *Endphase* 637, 641  
   *Protokollierungsphase* 640  
   *Protokollphase* 636  
   *RFC-Basisszenario* 637  
   *Rollenbau-Szenario* 646  
   *Setup* 637  
 UI-Komponente 488, 500, 503,  
 506, 517  
 UME 437, 447, 451, 813  
   *Architektur* 440  
   *Benutzer* 451  
   *Benutzeroberfläche* 441  
   *Datenquelle* 439, 443  
   *Import- und Exportfunktion* 439  
   *Sicherheitseinstellung* 439  
 UME-Aktion 446, 447, 451, 813  
 UME-Funktionen 438  
 UME-Gruppe 446, 448, 451, 456,  
 574, 813  
 UME-Konfiguration 442, 454  
 UME-Rolle 446, 451, 454, 455, 813  
 Unified Connectivity → UCON  
 unkritische Berechtigungen 135, 813  
 Unterdrückung der Berechtigungs-  
 prüfung 250  
 Unternehmensorganisation 98, 705,  
 813

Unterordner 622  
 Unterstellungsverhältnis 79  
 Untrusted RFC 742  
 Upgrade 813  
   *Berechtigungen* 259, 272  
   *Kosten* 256  
   *Projekt* 278  
   *Rolle* 259, 272  
   *Teilprojekt Berechtigungen* 38  
 User 813  
 User Access Management → UAM  
 User Lifecycle Management 345, 813  
 User Management Engine → UME  
 User\_Sessions in RBAC 53

## V

---

Variablen 596, 599  
 Veränderungshistorie in SAP ID  
   Management 368  
 Verantwortungsbereich 813  
 Verfahrensverzeichnis 130  
   *Datenschutz* 133  
 Verfügbarkeitskontrolle 130  
 Verkäufergruppe 537, 813  
   *Customizing* 719  
 Verkaufsbelegart im Verkaufsprozess  
   147  
 Verkaufsorganisation 108, 537, 813  
   *Customizing* 719  
 Verkaufsprozess 145  
   *Angebot* 146  
   *Auftrags erfassung* 146  
   *Buchungskreis* 146  
   *Debitor* 145  
   *Faktura* 148  
   *Konditionen* 146  
   *Kunde* 145  
   *Liefersperre* 148  
   *Lieferung* 147  
   *Sparte* 146  
   *Verkaufsbelegart* 147  
   *Verkaufsorganisation* 146  
   *Vertriebsweg* 146  
   *Zahlungseingang* 149  
 Verrichtung 39, 80  
   *Berechtigungskonzept* 88  
 Versand 732

Verteilung von Benutzerdaten in SAP  
   Identity Management 374  
 vertragliche Normen  
   *Definition* 116  
   *Regelkonformität* 114  
 Vertragsverhältnis  
   *Berechtigungen* 344  
 Vertretungsregelung in SAP ID  
   Management 381  
 Vertriebsauftragsart  
   *Customizing* 732  
   *Risiko* 732  
 Vertriebsorganisation 542  
 Vertriebsweg 108  
   *Customizing* 720  
   *Verkaufsprozess* 146  
 Vieraugenprinzip 813  
   *asymmetrisches* 693  
   *Benutzer- und Berechtigungs-*  
     *administration* 784  
   *Debitor* 146  
   *Debitorenbuchhaltung* 693  
   *Kreditor* 152  
   *symmetrisches* 693  
 View 492, 501  
 Vorgangsart 541, 581  
 Vorschlagsnutzung 391  
 Vorschlagswert 389, 391, 500, 502  
   *normativer Nutzen* 259  
   *Regelkonformität* 260  
   *Standardtransaktionen* 259  
   *Tabellen und ihre Relation* 253  
   *Ziel* 259

## W

---

Wareneingang im Beschaffungsprozess  
   151, 154  
 Warenversender 571  
 Warenzusteller 570  
 Web Dynpro 441, 443  
 Web Dynpro für ABAP 572  
 Web Intelligence → SAP BusinessOb-  
   jects  
 Webservices 165  
 Weitergabekontrolle 130  
 Werk 107, 814  
   *Customizing* 719

Workflow 814  
   *Benachrichtigungseinstellung* 363

## X

---

X-509 660

## Z

---

Zahllauf 149, 151, 814  
   *Finanzwesen* 702  
 Zahlungseingang im Verkaufsprozess  
   149  
 Zahlungsprogramm im Finanzwesen  
   702

ZBV 348, 814  
   *Definition* 349  
   *logisches System* 350  
   *Organisationsmanagement* 356  
   *SAP Access Control* 357  
   *Tochtersystem* 351  
   *UAM* 357, 358  
   *zentraler Pflegemandant* 350  
 Zentrale Benutzerverwaltung → ZBV  
 zentraler Pflegemandant (ZBV) 350  
 Ziel-ID 520, 521, 524  
 Zugangskontrolle 131  
 Zugriffsberechtigung 621, 622  
   *vordefinierte* 623  
 Zugriffskontrolle 131  
 Zuordnungsblock 490, 491, 495, 814  
 Zutrittskontrolle 130



Volker Lehnert, Katharina Stelzner, Anna Otto, Peter John

## SAP-Berechtigungen – Konzeption und Realisierung

847 Seiten, gebunden, 3. Auflage 2016  
79,90 Euro, ISBN 978-3-8362-3768-0

 [www.sap-press.de/3849](http://www.sap-press.de/3849)



**Volker Lehnert** ist seit 2000 bei SAP in unterschiedlichen Positionen in den Bereichen Compliance und Sicherheit tätig.

**Katharina Stelzner** (geb. Bonitz) arbeitet seit 2006 als Technologieberaterin für die SAP Deutschland AG.

**Anna Otto** arbeitet seit 2007 als GRC-Beraterin für die SAP Deutschland AG und war zwischenzeitlich ebenfalls als GRC-Beraterin für die SAP (Schweiz) AG tätig.

**Dr. Peter John** hat das neue Konzept der Analyseberechtigungen als Nachfolger der vorherigen Reportingberechtigungen in BW entworfen und entwickelt.

*Wir hoffen sehr, dass Ihnen diese Leseprobe gefallen hat. Sie dürfen sie gerne empfehlen und weitergeben, allerdings nur vollständig mit allen Seiten. Bitte beachten Sie, dass der Funktionsumfang dieser Leseprobe sowie ihre Darstellung von der E-Book-Fassung des vorgestellten Buches abweichen können. Diese Leseprobe ist in all ihren Teilen urheberrechtlich geschützt. Alle Nutzungs- und Verwertungsrechte liegen beim Autor und beim Verlag.*

Teilen Sie Ihre Leseerfahrung mit uns!

