Berechtigungen in SAP S/4HANA und SAP Fiori

Umfassendes Handbuch zum Berechtigungswesen in SAP S/4HANA

Kapitel 2
Technische Elemente der SAP-Berechtigungsverwaltung

Die technischen Elemente der Berechtigungsverwaltung bleiben in SAP S/4HANA im Vergleich zu SAP ECC im Wesentlichen unverändert. Neu sind die Fiori-Entitäten und die CDS-Views. Dieses Kapitel nimmt sowohl die klassischen als auch die neuen Elemente in den Blick.

Im SAP-Berechtigungswesen gibt es technische Elemente, die Ihnen im Tages- und Projektbetrieb immer wieder begegnen werden. Auch in diesem Buch werden diese im Kontext von verschiedenen Themen häufig erwähnt. Daher werden in diesem Abschnitt, an Kapitel 1, »Grundlagen«, anknüpfend, die grundlegenden technischen Elemente der SAP-Berechtigungsverwaltung aufgeführt und erklärt.

In Abschnitt 2.1 werden Rollenarten, Berechtigungsprofile, Menüobjekte und Berechtigungsobjekte erklärt. In Abschnitt 2.2 erfahren Sie mehr über die Komponenten des Benutzerstammsatzes, Benutzertypen und ihre Verwendung sowie über die Funktionsweise des Single Sign-on.

In Abschnitt 2.3 stellen wir die wichtigsten Customizing-Einstellungen für die Benutzer- und Berechtigungsverwaltung vor. In Abschnitt 2.4 erhalten Sie eine Beschreibung der einzelnen Schritte in der Transaktion SU25. In Abschnitt 2.5 lernen Sie CDS-Views kennen. In Abschnitt 2.6 werden unterschiedliche Berechtigungstraces beschrieben.

2.1 Rollenverwaltung

Bedeutung der Rollen

Rollen sind ein zentrales Element im SAP-Berechtigungskonzept (siehe Abschnitt 1.1, »Was sind SAP-Berechtigungen?«). Um SAP-Transaktionen auszuführen und Geschäftsobjekte abzurufen, benötigen Benutzer passende Berechtigungen. Die Berechtigungen sind in Rollen zusammengefasst. Die Benutzeradministration weist die entsprechenden Rollen unter der Verwendung des Benutzerstammsatzes zu, sodass die Benutzer die für ihre Aufgaben passenden Transaktionen und Applikationen verwenden können (siehe Abbildung 2.1).

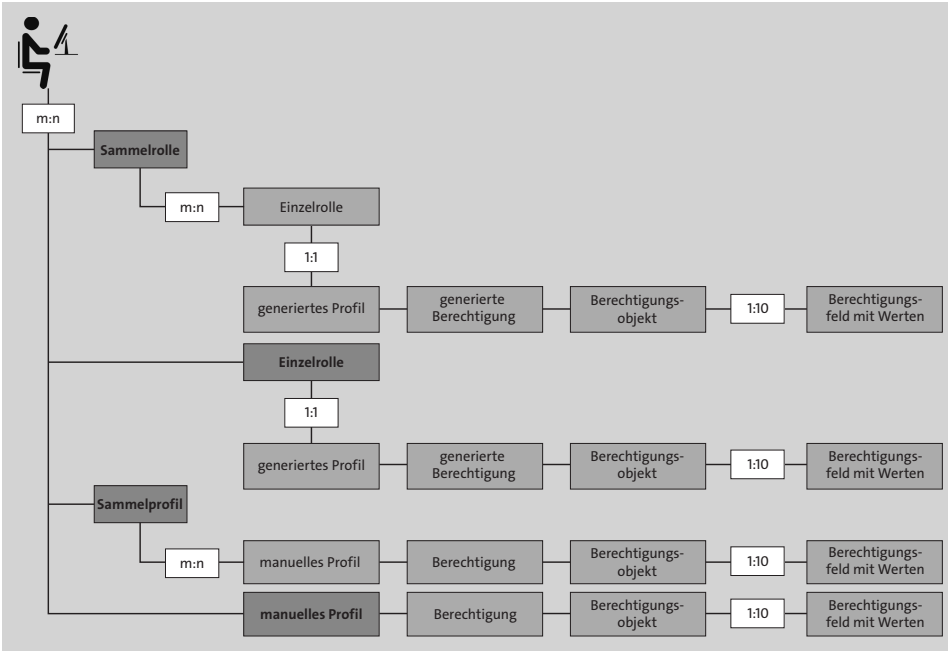


Abbildung 2.1 Berechtigungselemente in SAP

In den folgenden Abschnitten beschreiben wir die einzelnen Berechtigungselemente, die in Abbildung 2.1 dargestellt sind. Wie Sie Einzel- und Sammelrollen erstellen, lesen Sie in Abschnitt 6.2, »Einzel- und Sammelrollen anlegen und pflegen«.

2.1.1 Rollen

Rollen werden in der Transaktion PFCG (Profilgenerator) angelegt. Beim Anlegen einer Rolle kann zwischen Einzelrollen und Sammelrollen ausgewählt werden.

Einzelrollen

Eine *Einzelrolle* wird gemäß einer Namenskonvention angelegt (siehe Abschnitt 6.1, »Eine Namenskonvention für Rollen festlegen«) und setzt sich aus den folgenden Bestandteilen zusammen (siehe Abbildung 2.2):

❶ der Beschreibung der Rolle

❷ dem Menü

❸ den Berechtigungen

❹ der Benutzerzuweisung

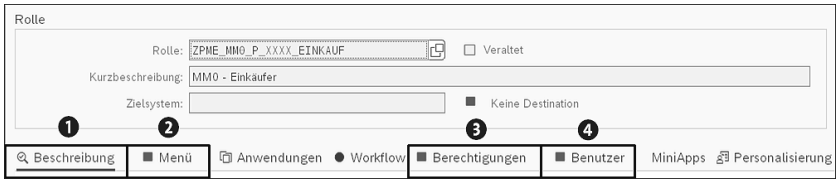


Abbildung 2.2 Beispiel für eine Einzelrolle

Sammelrollen

Eine *Sammelrolle* setzt sich aus mehreren Einzelrollen zusammen. Sammelrollen (siehe auch Abschnitt 6.2.3, »Sammelrolle anlegen«) werden für die bessere Strukturierung der Einzelrollen verwendet.

In Sammelrollen selbst können keine Anpassungen an den Berechtigungen durchgeführt werden. Solche Änderungen können nur in Einzelrollen vorgenommen werden. Den Benutzern werden die Einzelrollen innerhalb der Sammelrollen zugewiesen. Diese Art der Rollenzuweisung heißt *indirekte Rollenzuweisung* (siehe Abbildung 2.3).

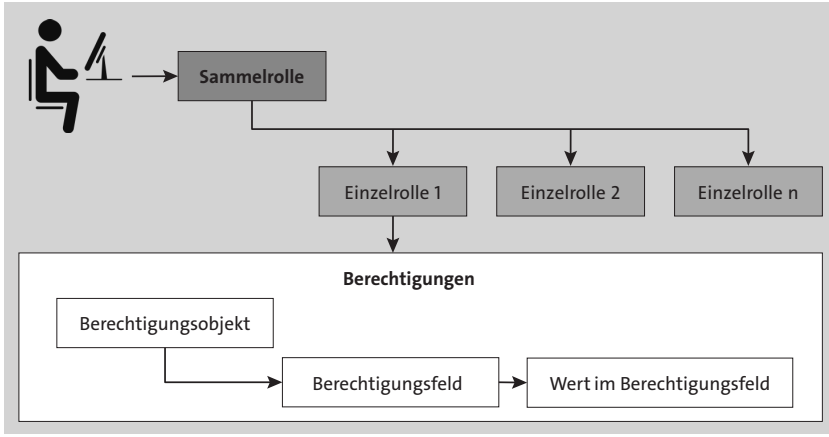


Abbildung 2.3 Indirekte Rollenzuweisung bei Sammelrollen

Masterrollen und abgeleitete Rollen

Außerdem wird zwischen Masterrollen (auch Referenzrollen oder Mutterrollen genannt) und abgeleiteten Rollen unterschieden.

Masterrollen sind die Einzelrollen, die Anwendungen enthalten und die für Nutzer mit der gleichen Jobfunktion vom Grundprinzip her gleich sind. Sie müssen sich aber in einer oder mehreren Feldausprägungen der Organisationsfelder unterscheiden, z. B. im Personalbereich oder Buchungskreis. Die Masterrolle liefert dann die Vorlage für alle abgeleiteten Rollen, in die wiederum die Organisationsebenen hinterlegt werden.

Masterrollen werden als normale Einzelrollen in der Transaktion PFCG angelegt, und technisch gesehen werden sie erst dann zu Masterrollen,

wenn eine abgeleitete Rolle mit der Referenz zu dieser Rolle angelegt wird (siehe Abbildung 2.4).

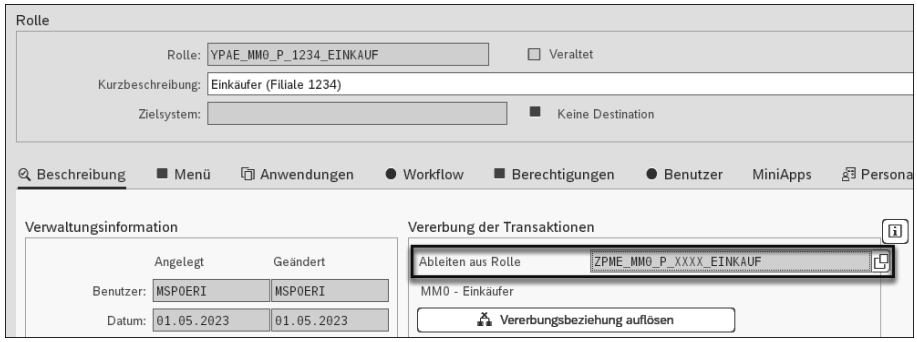


Abbildung 2.4 Beispiel für eine abgeleitete Rolle

Änderungen an Masterrollen

Wenn Sie Änderungen an einer Masterrolle vornehmen, werden diese über eine *Vererbung* in alle abgeleiteten Rollen übertragen. Alle abgeleiteten Rollen werden gleichzeitig überschrieben. Lediglich in den Feldern, die als Organisationsebenen definiert sind und nur in den jeweiligen abgeleiteten Rollen gepflegt werden können, herrscht eine Ausnahme. Viele Organisationen verwenden Masterrollen und abgeleitete Rollen, um den Aufwand für die Pflege des Rollenkonzepts im SAP-System zu reduzieren (siehe Abbildung 2.5). Mehr Informationen zu Ableitungen finden Sie in Abschnitt 6.2.2, »Rolle ableiten«.

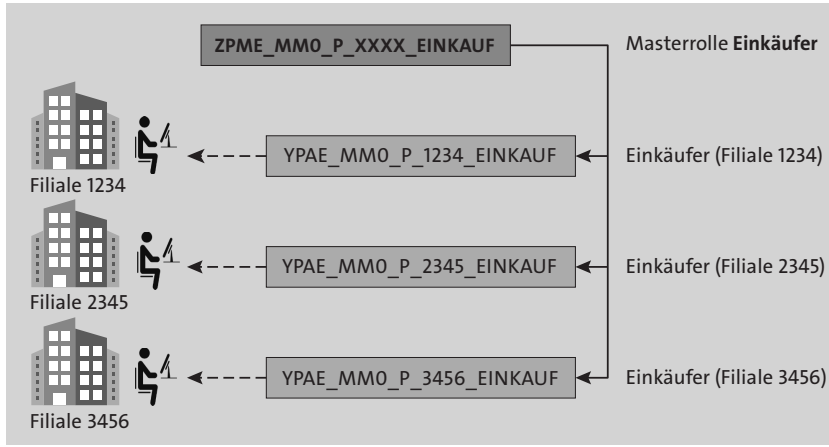


Abbildung 2.5 Masterrollen und abgeleitete Rollen

Namen der Masterrollen

Wir empfehlen, ein Merkmal für die Masterrollen in der Namenskonvention zu definieren. Im Beispiel in Abbildung 2.4 fängt der Name der Masterrolle mit Z an, der Name der abgeleiteten Rolle fängt mit Y an.

Darüber hinaus werden die Organisationsebenen in den Masterrollen mit sogenannten *Dummy-Werten*, wie beispielweise $ oder @, ausgeprägt. Die Masterrollen sollten keinen Benutzern zugewiesen werden. Sollten sie den Benutzern aus Versehen zugewiesen werden, funktionieren sie auf Grund der Dummy-Werte in den Organisationsebenen nicht.

2.1.2 Profile

Profile der Rollen und Sammelprofile

Profile sind die Objekte, die die Berechtigungsdaten tatsächlich speichern. Rollen sind wiederum Container, die die Profile enthalten. Beim Anlegen der Einzelrollen wird für jede Rolle ein Profil generiert. Ohne die generierten Profile funktionieren die Rollen nicht. Somit gibt es im System für jede Einzelrolle ein Profil.

Darüber hinaus gibt es sogenannte *Sammelprofile*. Die bekanntesten Sammelprofile sind die Profile SAP_ALL und SAP_NEW. Außerdem liefert SAP eine Vielzahl anderer Sammelprofile, die im Tages- und Projektbetrieb seltener Verwendung finden.

Profil SAP_ALL

Das Profil SAP_ALL enthält alle vorhandenen Berechtigungen im SAP-System außer dem Berechtigungsobjekt S_RFCACL (Berechtigungsprüfung für RFC-Benutzer). In SAP ECC kann man mit dem Profil SAP_ALL alle Berechtigungen im System zuweisen. In SAP S/4HANA brauchen Benutzer zusätzliche Berechtigungen für Fiori-Entitäten und das Berechtigungsobjekt S_RFCACL, um auf das SAP Fiori Launchpad und auf Fiori-Apps zugreifen zu können.

Profil SAP_NEW

Das Profil SAP_NEW ist ein Sammelprofil zur Überbrückung der Release-Unterschiede bei neuen oder geänderten Berechtigungsprüfungen für bestehende Funktionen. Dieses Sammelprofil enthält sehr umfangreiche Berechtigungen, da die Organisationsebenen beispielsweise mit der vollen Berechtigung (*) ausgeprägt sind.

2.1.3 Menüobjekte

Ordner im Menü der Rolle

Die Registerkarte **Menü** wird hauptsächlich zum Erstellen der Rolle auf Transaktions- und Applikationsebene verwendet. Dies ist der erste Schritt, um die Rolle mit Berechtigungen auszustatten, die es Benutzern ermöglichen, eine oder mehrere Aufgaben im System zu erledigen. Darüber hinaus können dem Menü Ordner hinzugefügt werden. Mit deren Hilfe können Transaktionen angeordnet werden. Dies bestimmt, wie die Transaktionen auf dem Startbildschirm der Benutzer angezeigt werden, wenn Sie sich in SAP GUI anmelden (siehe Abbildung 2.6).

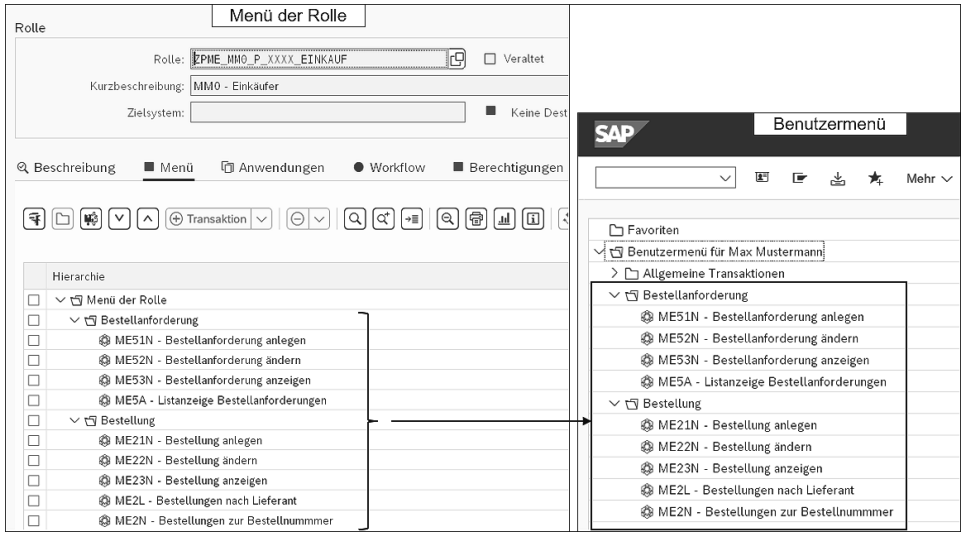


Abbildung 2.6 Beispiel für ein Benutzer-Menü

Wenn das SAP Fiori Launchpad zum Einstiegspunkt ins SAP-System für Endanwender*innen wird, besteht keine administrative Notwendigkeit, Ordner in Rollenmenüs zu pflegen. Bei manchen Organisationen werden die Transaktionen auch nicht mehr im Menü der Rollen der Benutzer hinzugefügt.

Transaktionen

Im Menü der Einzelrollen in SAP S/4HANA werden hauptsächlich Fiori-Entitäten und Transaktionen hinzugefügt. *Transaktionen* sind Programme, die innerhalb eines SAP-Systems durch Benutzer oder automatisierte Abläufe aufgerufen werden. Es handelt sich dabei um den funktionalen Bestandteil eines SAP-Systems, über den Daten in der SAP-Datenbank verändert werden. Jede SAP-Transaktion hat einen Transaktionscode. Dieser besteht aus Buchstaben und/oder Zahlen, die die Benutzer in das Befehlsfeld eingeben, um die Transaktion aufzurufen. Diese Transaktionscodes werden im Menü der Rollen hinzugefügt, damit Benutzer, die diese Rollen zugewiesen bekommen, sie in SAP GUI aufrufen können (siehe Abbildung 2.6).

Fiori-Entitäten

Dem Menü der Rolle können folgende *Fiori-Entitäten* zugewiesen werden:

- Launchpad-Kataloge
- Launchpad-Gruppen
- Launchpad-Spaces (Bereiche)

In Abschnitt 1.7.2., »Berechtigungsprüfung für Fiori-Apps«, werden diese Fiori-Entitäten beschrieben.

Andere Menü-Objekte

Neben den Transaktionen und Fiori-Entitäten gibt es weitere verschiedene Objekte, die dem Menü der Rolle in Transaktion PFCG hinzugefügt werden

können, wie z. B. Web-Dynpro-Anwendungen, URLs, Berechtigungsvorschlagswerte für RFC-Funktionsbausteine und OData-Services.

2.1.4 Berechtigungsobjekte

Zweck von Berechtigungsobjekten

Berechtigungsobjekte ermöglichen komplexe Tests der Berechtigungen für mehrere Bedingungen. Ein Berechtigungsobjekt fasst bis zu zehn UND-verknüpfte Felder zusammen. Berechtigungen ermöglichen es Benutzern, Aktionen innerhalb des Systems auszuführen. Für eine erfolgreiche Berechtigungsprüfung müssen alle zur Ausführung der Aktion erforderlichen Berechtigungsobjekte und -werte entsprechend in der Rolle eingetragen sein.

Klassen und Feldwerte

Die Berechtigungsobjekte sind zur Verständlichkeit in Klassen eingeteilt. Eine Klasse ist eine logische Zusammenfassung von Berechtigungsobjekten und entspricht z. B. einem Anwendungsbereich (Finanzbuchhaltung, Personalwesen usw.). Die Feldwerte in Berechtigungsobjekten sind mit den im ABAP Dictionary hinterlegten Datenelementen verbunden.

Beispiel für die Funktionsweise von Berechtigungsobjekten

Um die Funktionsweise der *Berechtigungsobjekte* zu verstehen, schauen wir uns ein Beispiel der Berechtigungsobjekte, die für die Ausführung der Transaktion MM01 (Material anlegen) notwendig sind, an. Wenn wir die Transaktion MM01 im Menü der Rolle hinzufügen, werden die im Kontext der Transaktion MM01 in der Transaktion SU24 gepflegten Berechtigungsobjekte und -werte automatisch in die Rolle hinzugefügt (siehe Abbildung 2.7).

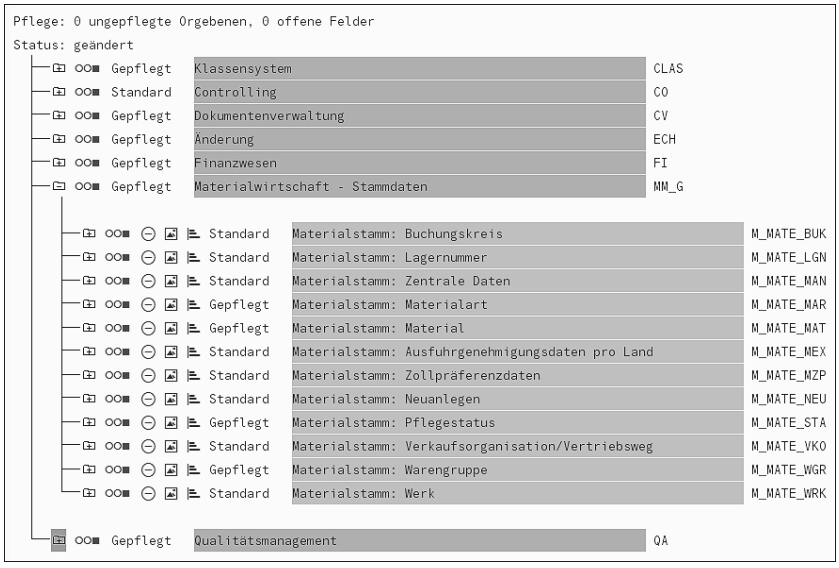


Abbildung 2.7 Beispiel für Berechtigungsobjekte für die Transaktion MM01 in der Rolle in Transaktion PFCG

Schauen wir uns drei Berechtigungsobjekte (M_MATE_BUK, M_MATE_MAT und M_MATE_STA) der Klasse MM_G – Materialwirtschaft – Stammdaten – an (siehe Abbildung 2.8).

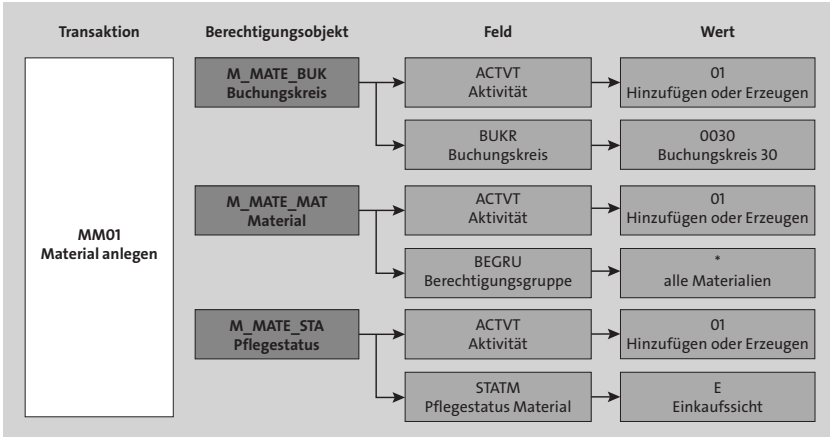


Abbildung 2.8 Beispiel für Berechtigungsobjekte der Klasse MM_G für die Transaktion MM01

Berechtigungsobjekt M_MATE_BUK

Das Berechtigungsobjekt M_MATE_BUK (Materialstamm: Buchungskreis) enthält zwei Felder: **ACTVT** (Aktivität) und **BUKRS** (Buchungskreis). In unserem Beispiel ist der Wert des Felds **ACTVT** »01« (Hinzufügen oder Erzeugen) und der Wert des Felds **BUKRS** »0030« (Buchungskreis 0030). Das bedeutet, dass diese Berechtigung die Anlage des Materialstamms für Buchungskreis 0030 ermöglicht. Der Wert 01 (Hinzufügen oder Erzeugen) wurde automatisch in die Rolle gezogen, weil er der Funktion der Transaktion MM01 (Material anlegen) entspricht. **BUKRS** (Buchungskreis) ist eine Organisationsebene, die in der Rolle gepflegt wird.

Berechtigungsobjekt M_MATE_MAT

Das Berechtigungsobjekt M_MATE_MAT (Materialstamm: Material) enthält zwei Felder: **ACTVT** (Aktivität) und **BEGRU** (Berechtigungsgruppe). In unserem Beispiel ist der Wert im Feld **ACTVT** »01« (Hinzufügen oder Erzeugen) und der Wert im Feld **BEGRU** ist »*«. Der Wert »*« bedeutet, dass für alle Berechtigungsgruppen ein Materialstamm angelegt werden kann.

Feld »Berechtigungsgruppe«

Das Feld **BEGRU** (Berechtigungsgruppe) ist in mehreren Geschäftsobjekten vorhanden, z. B. im Geschäftspartner und in Stücklisten in SAP. Das Feld dient der feinen Steuerung von Berechtigungen für Objekte. Die Nutzung des Felds **BEGRU** ist optional. Allerdings wird das Objekt mit diesem Feld, unabhängig davon, ob das Feld **BEGRU** im aufgerufenen Objekt (z. B. Materialstamm) ausgefüllt ist, bei der Ausführung der Transaktionen geprüft. Deswegen muss das Berechtigungsobjekt M_MATE_MAT ausgeprägt sein, damit die Benutzer die Transaktion MM01 ausführen können.

Berechtigungsobjekt M_MATE_STA

Berechtigungsobjekt M_MATE_STA (Materialstamm: Pflegestatus) enthält zwei Felder: **ACTVT** (Aktivität) und **STATM** (Pflegestatus Materialstammsatz). In unserem Beispiel ist der Wert für das Feld **ACTVT** »01« (Hinzufügen oder Erzeugen), und der Wert für **STATM** ist »E«. Das Feld **STATM** entspricht den sogenannten *Sichten* im Materialstamm. Der Wert »E« entspricht der Einkaufssicht. Das bedeutet, dass Benutzer mit dieser Berechtigung eine Einkaufssicht im Materialstamm anlegen können (siehe Abbildung 2.9).

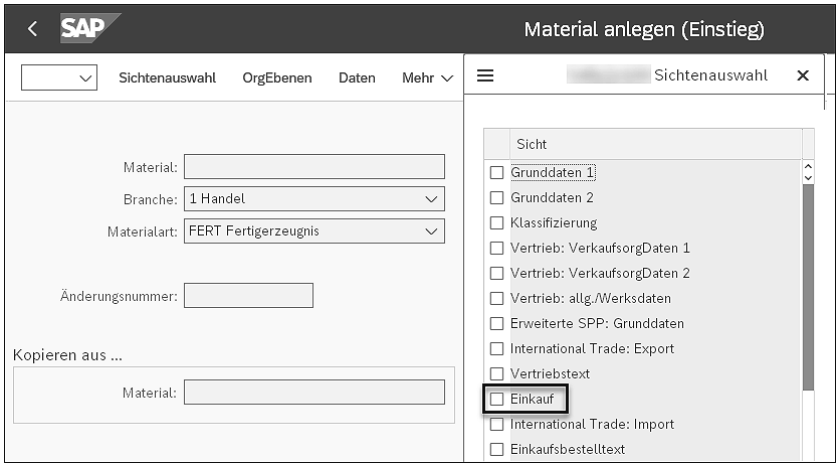


Abbildung 2.9 Transaktion MM01: Sichten im Materialstamm

Berechtigungen werden summiert

Die Berechtigungen, die den Benutzern mit mehreren Rollen zugewiesen sind, werden im *Benutzerprofil* zusammengefasst.

Nehmen wir unser Beispiel mit der Transaktion MM01. Stellen wir uns vor, dass ein Benutzer in einer Rolle die folgende Ausprägung der Berechtigungsobjekte hat:

- M_MATE_BUK, **ACTVT** = »01, 02, 03«; **BUKRS** = »0030« (Buchungskreis)

M_MATE_STA, **ACTVT** = »01, 02, 03« **STATM** = »E« (Einkauf)

- In einer anderen Rolle hat der Benutzer die folgende Ausprägung dieser Berechtigungsobjekte:
- M_MATE_BUK, **ACTVT** = »01, 02, 03«; **BUKRS** = »0040« (Buchungskreis)
- M_MATE_STA, **ACTVT** = »01, 02, 03«; **STATM** = »E« (Einkauf), V (Vertrieb)

Die Berechtigungen summieren sich nun, das bedeutet, dass der Benutzer die Berechtigung hat, sowohl die Vertriebssicht für den Buchungskreis 0040 als auch für den Buchungskreis 0030 anzulegen und zu pflegen.

2.2 Benutzerverwaltung

Mit der *Benutzerverwaltung* legt die Benutzeradministration für alle Anwender*innen einen Benutzerstammsatz an, damit diese sich am SAP-System anmelden können. Über den Benutzerstammsatz ordnet die Benutzeradministration die für die Funktion des Benutzers vorgesehenen Rollen im SAP-System zu. So wird festgelegt, welche Aktivitäten im Benutzermenü bzw. welche Fiori-Apps auf dem SAP Fiori Launchpad enthalten sind und mit welchen Berechtigungen der Benutzer ausgestattet ist.

2.2.1 Benutzerstammsatz

Komponenten des Benutzerstammsatzes

Der *Benutzerstammsatz* enthält alle Details von Benutzern wie Adressdaten, Funktion, Benutzergruppe, zugewiesene Berechtigungen, Benutzerlizenztyp und weitere Daten, die Sie in den in Abbildung 2.10 markierten Registerkarten finden. Mit der Transaktion SU01 oder SU01D können Sie die Details einsehen.

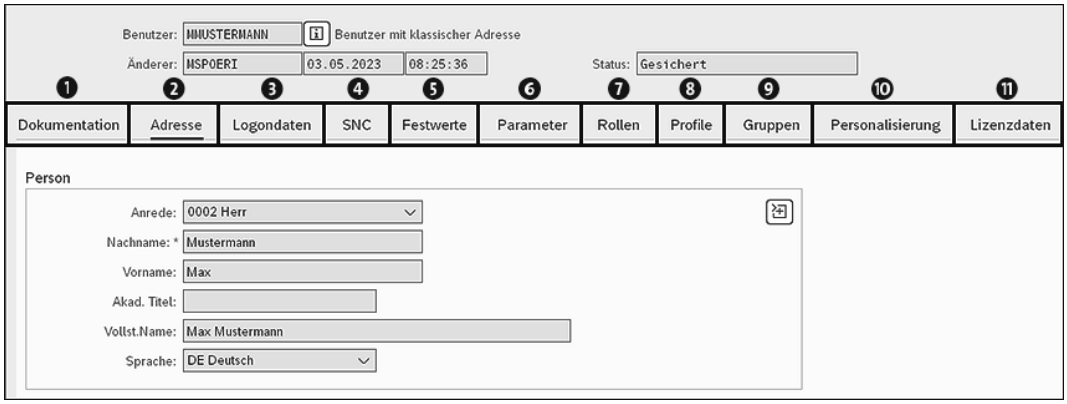


Abbildung 2.10 Beispiel für einen Benutzerstammsatz in der Transaktion SU01D

Die einzelnen Komponenten des Benutzerstammsatzes sind:

❶ **Dokumentation**
Auf dieser Registerkarte kann die Benutzeradministration manuell Einträge erfassen.

❷ **Adresse**
Diese Registerkarte enthält alle Adressdaten des Benutzers, wie persönliche Daten, Kommunikationsdaten und die Firmenadresse.

❸ **Logondaten**
Hier werden der Benutzertyp, der Gültigkeitszeitraum und die Kostenstelle gespeichert.

❹ **SNC**
SNC bedeutet *Secure Network Communications*. SNC ist eine Softwareschicht in der SAP-Systemarchitektur, die eine Schnittstelle zu einem externen Sicherheitsprodukt bereitstellt.

❺ **Festwerte**
Diese Registerkarte enthält das Default-Startmenü, den Default-Drucker, die Anmeldesprache, die Dezimaldarstellung, die Datumsdarstellung und anderes.

❻ **Parameter**
Diese Registerkarte enthält die Standardparameter, die dem Benutzer zugewiesen sind.

❼ **Rollen**
Diese Registerkarte enthält die Rollen, die dem Benutzer zugewiesen sind.

❽ **Profile**
Diese Registerkarte enthält sowohl Profile der zugewiesenen Rollen als auch dem Benutzer direkt zugewiesene Profile (z. B. Profil SAP_ALL).

❾ **Gruppen**
Auf dieser Registerkarte können dem Benutzer eine oder mehrere Gruppen zugeordnet werden. Die Einteilung von Benutzern in Benutzergruppen auf der Registerkarte **Gruppen** dient vor allem zur Gruppierung von Benutzern für die Massenpflege mit der Transaktion SU10.

❿ **Personalisierung**
Auf dieser Registerkarte wird die Personalisierung des Benutzers gespeichert.

⓫ **Lizenzdaten**
Auf dieser Registerkarte wird der vertragliche Benutzertyp gespeichert.

Die Pflege des Benutzerstamms wird in Abschnitt 10.1, »Benutzer im SAP-System anlegen und pflegen«, im Detail beschrieben.

Die ZBV für die Benutzerverwaltung nutzen

Die Benutzerstammsätze sind mandantenabhängig. Daher müssen Sie für jeden Mandanten im SAP-System eigene Benutzerstammsätze pflegen. Um die system- und mandantenübergreifende Benutzerverwaltung zu vereinfachen, können Sie die *Zentrale Benutzerverwaltung* (ZBV) einsetzen. Die Pflege der zentral verwalteten Benutzer weicht leicht von der Benutzerverwaltung ohne ZBV ab (siehe Abschnitt 10.3, »Benutzer in der zentralen Benutzerverwaltung (ZBV) pflegen«).

Sie können die Benutzerstammsätze nicht transportieren. Stattdessen können Sie diese mit dem Mandantenkopierer kopieren, oder Sie verwenden die Zentrale Benutzerverwaltung und verteilen damit die Benutzerstammsätze des Zentralsystems an die Tochtersysteme.

2.2.2 Benutzertypen

Zweck von unterschiedlichen Benutzertypen

Benutzer im SAP-System werden für unterschiedliche Zwecke angelegt. Daher gibt es unterschiedliche Typen von Benutzern. Dies ist erforderlich, um unterschiedliche Sicherheitsrichtlinien für diese unterschiedlichen Benutzertypen festzulegen. Beispielsweise kann Ihre Richtlinie festlegen, dass Anwender*innen (Dialogbenutzer*innen), die ihre Aufgaben interaktiv ausführen, ihre Kennwörter regelmäßig ändern müssen, während technische Benutzer, die Jobs im Hintergrund ausführen (Systembenutzer), dies nicht tun müssen.

Der Benutzertyp wird bei der Anlage des Benutzerstammsatzes ausgewählt (siehe Abbildung 2.11). Technisch gesehen ist es möglich, den Benutzertyp eines existierenden Benutzers zu ändern. Allerdings verbieten die SAP-Sicherheitsrichtlinien von vielen Organisationen dies meist.

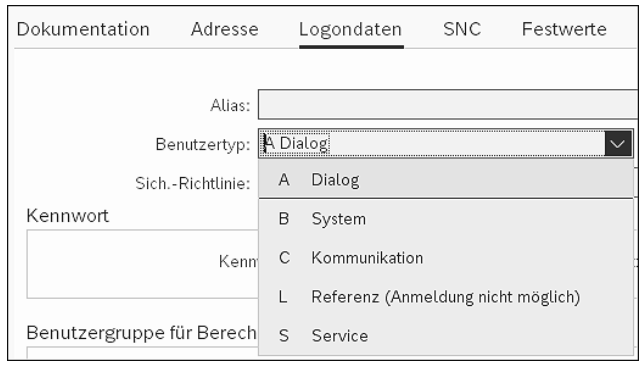


Abbildung 2.11 Transaktion SU01: Auswählen des Benutzertyps

Verschiedene Benutzertypen

Es gibt fünf Benutzertypen in SAP-Systemen, die in den folgenden Abschnitten vorgestellt werden.

Der Dialogbenutzer (A Dialog)

Ein normaler *Dialogbenutzer* wird von einer Person für alle Anmeldearten verwendet. Bei der Dialoganmeldung erfolgt die Prüfung auf abgelaufene/initiale Passwörter mit der Möglichkeit zur eigenen Passwortänderung. Mehrfache Dialoganmeldungen werden überprüft und gegebenenfalls protokolliert.

Der Systembenutzer (B System)

Verwenden Sie den *Systembenutzertyp* für systeminterne (Hintergrundverarbeitung) und systembedingte Vorgänge (Application Link Enabling (ALE), Workflow, Transport Management System (TMS), ZBV). Eine Dialoganmeldung (mittels SAP GUI) ist nicht möglich.

Ein Benutzer dieses Typs ist von den allgemeinen Einstellungen zur Gültigkeitsdauer eines Passworts ausgeschlossen. Das Passwort kann nur durch die Benutzeradministration über die Transaktion SU01 geändert werden. Eine Mehrfachanmeldung ist zulässig.

Der Kommunikationsbenutzer (C Kommunikation)

Der *Kommunikationsbenutzer* wird für die dialogfreie Kommunikation mit den Systemen verwendet. Eine Dialoganmeldung (mittels SAP GUI) ist nicht möglich.

Ein Benutzer dieses Typs unterliegt prinzipiell den allgemeinen Einstellungen zur Gültigkeitsdauer eines Passworts und ist (wie ein Dialogbenutzer) in der Lage, sein Passwort zu ändern. Hierbei müssen die Dialoge zur Passwortänderung vom Aufrufer zur Verfügung gestellt werden.

Der Servicebenutzer (S Service)

Ein Benutzer vom Typ **Service** ist ein Dialogbenutzer, der einem anonymen, größeren Nutzerkreis zur Verfügung steht. In der Regel sollten nur stark eingeschränkte Berechtigungen vergeben werden.

Servicebenutzer werden z. B. für anonyme Systemzugänge über einen öffentlichen Webservice verwendet. Nach einer individuellen Authentifizierung kann eine mit einem Servicebenutzer begonnene anonyme Sitzung als personenbezogene Sitzung unter einem Dialogbenutzer weitergeführt werden.

Bei der Anmeldung erfolgt keine Prüfung auf abgelaufene/initiale Passwörter. Nur die Benutzeradministration kann das Passwort ändern. Eine Mehrfachanmeldung ist zulässig. Aus diesen Gründen wird dieser Benutzertyp oft für Testbenutzer in Testsystemen verwendet.

Nicht alle Funktionen können mit Servicebenutzern getestet werden

Sie sollen beachten, dass (wie bei den Dialogbenutzern) nicht alle Funktionen mit Servicebenutzern getestet werden können. Beispielsweise kann der Zugriff auf GOS-Anhänge (Generic Object Services) mit Servicebenutzern nicht getestet werden.

Der Referenzbenutzer (L Referenz)

Ein *Referenzbenutzer* ist wie der Servicebenutzer ein allgemeiner, nicht personenbezogener Benutzer. Mit einem Referenzbenutzer kann man sich nicht anmelden. Der Referenzbenutzer dient nur der zusätzlichen Vergabe von Berechtigungen. Auf der Registerkarte **Rollen** können Sie für Dialogbenutzer einen Referenzbenutzer für zusätzliche Rechte angeben.

Eine Übersicht der Eigenschaften der verschiedenen Benutzertypen sehen Sie in Tabelle 2.1.

Eigenschaft/ Benutzertyp	Dialog	Kommunikation	System	Service	Referenz
Dialoganmeldung (SAP GUI)	X	–	–	X	–
Passwortänderung	X	X	–	–	–

Tabelle 2.1 Eigenschaften verschiedener Benutzertypen

Außer den Referenzbenutzern sind alle anderen Benutzertypen generell in der Lage, sich per RFC an einem System anzumelden oder Hintergrundjobs auszuführen.

2.2.3 Single Sign-on

Definition von »Single Sign-on«

Mit einem sogenannten *Single Sign-on* (SSO) können sich Benutzer bei mehreren Anwendungen mit nur einem einzigen Passwort anmelden, da die Authentifizierung mithilfe eines digitalen Tokens funktioniert. Nach einer einmaligen Identifikation haben die Benutzer Zugriff auf alle Dienste ihrer Organisation, für die sie zuvor berechtigt wurden. Auf diese Weise müssen sich die Anwender*innen nur noch ein einziges Passwort statt viele für unterschiedliche Anwendungen merken, sodass der Aufwand für vergessene Passwörter und entsprechendes Zurücksetzen der Passwörter minimiert wird.

Single Sign-on auf SAP Logon

Die Verwendung von Single Sign-on auf SAP Logon geschieht in mehreren Schritten: Zuerst muss das Profil der Zentralinstanz angepasst werden. Anschließend muss im SAP Logon ein Eintrag ausgewählt und die Secure Network Communication eingeschaltet werden. Zum Schluss muss in das Feld **SNC-Name** auf der Registerkarte **SNC** im Benutzerstammsatz (siehe Abbildung 2.10 in Abschnitt 2.2.1, »Benutzerstammsatz«) »p:< DN-Name des AS ABAP>« eingetragen werden.

Anbieter für Single Sign-on

Für Single Sign-on stehen zahlreiche Lösungen und Anbieter zur Verfügung, wobei die folgenden am weitesten verbreitet sind:

- Security Assertion Markup Language (SAML)
- Identity Provider, Microsoft Active Directory Federation Services (ADFS)
- Security Token Service (STS)

Jede dieser Komponenten hat einen anderen Fokus, sodass Organisationen aus einer Reihe möglicher Lösungsansätze auswählen und diese an die eigenen Anforderungen anpassen können.

2.3 Customizing und Einstellungen

Die wichtigsten Einstellungen im Customizing

Es gibt diverse Einstellungen für die Benutzer- und Berechtigungsverwaltung, die einen Einfluss auf das Berechtigungs- und Benutzermanagement haben und im SAP-System vorgenommen werden müssen oder können. Wir werden die einzelnen Einstellungen im Customizing in den entsprechenden Abschnitten in den folgenden Kapiteln dieses Buchs besprechen.

In diesem Abschnitt beschreiben wir die wichtigsten Einstellungen: die Pflege der Berechtigungsvorschlagwerte, das Ausschalten der Berechtigungsprüfungen und die Pflege der SAP-Standardtabellen zur Steuerung der Benutzer- und Berechtigungsverwaltung.

2.3.1 SAP-Vorschlagswerte

In Abschnitt 1.4, »Berechtigungen in SAP ECC« wurde bereits kurz erklärt, wie die Berechtigungsprüfungen im SAP-System funktionieren und woher die Berechtigungsvorschlagswerte kommen, die in den Profilgenerator gezogen werden.

In diesem Abschnitt erklären wir die Funktionsweise der Transaktionen SU25 und SU24 im Detail. In Abschnitt 11.1, »Arbeitsschritte im SU25-Abgleich«, und in Abschnitt 11.2, »Praxisübungen zur Anzeige und Pflege von Vorschlagswerten in der Transaktion SU24«, finden Sie Anleitungen zur Durchführung des SU25-Abgleichs sowie zur Pflege von Vorschlagswerten in der Transaktion SU24.

Arbeitsschritte für die Berechtigungsprüfung

In Abbildung 2.12 und im Folgenden sind die einzelnen Arbeitsschritte der Einrichtung einer Berechtigungsprüfung dargestellt.

❶ **ABAP Workbench**
Bei der Entwicklung der neuen Apps und Transaktionen in SAP definiert die Entwicklung mit dem AUTHORITY-CHECK-Befehl, welche Berechtigungsobjekte beim Aufruf dieser Apps oder Transaktionen geprüft werden.

❷ **Transaktion SU22**
Mit der Transaktion SU22 ordnet die Entwicklung den Transaktionen und Apps die Berechtigungsobjekte zu und bearbeitet die Berechtigungsvorschlagswerte der Berechtigungsobjekte.

❸ **Transaktion SU25**
Nach der Installation des Systems übernimmt die Berechtigungsadministration über die Transaktion SU25 die Berechtigungsvorschlagswerte aus den SAP-Tabellen (USOBX und USOBT) in die Kundentabellen (USOBX_C und USOBT_C).

❹ **Transaktion SU24**
Bei der Rollenpflege und dem Rollentest stellt die Berechtigungsadministration fest, dass die Berechtigungsvorschlagswerte für manche Transaktionen oder Applikationen fehlen oder dass manche Berechtigungsprüfungen ausgeschaltet werden sollen. Dies pflegt die Berechtigungsadministration in der Transaktion SU24 (Pflege von Berechtigungsvorschlagswerten).

❺ **Transaktion PFCG**
Beim Anlegen einer Rolle fügt die Berechtigungsadministration die Transaktionen und Apps dem Menü der Rolle hinzu. Die entsprechenden Berechtigungsobjekte für die Transaktionen und Apps werden aus den kundeneigenen Tabellen (USOBX_C und USOBT_C) in das Profil der Rolle gezogen. Die Berechtigungsadministration pflegt die offenen Felder in der Rolle und generiert das Profil.

❻ **SAP Fiori Launchpad/SAP GUI**
Die Endanwender*innen, deren Benutzern die Rolle zugewiesen ist, rufen die Transaktionen oder Apps auf, zu denen sie den Zugriff aus der Rolle bekommen haben. Dabei werden die Berechtigungsprüfungen durchgeführt, die im Programm in ❶ von der Entwicklung definiert wurden.

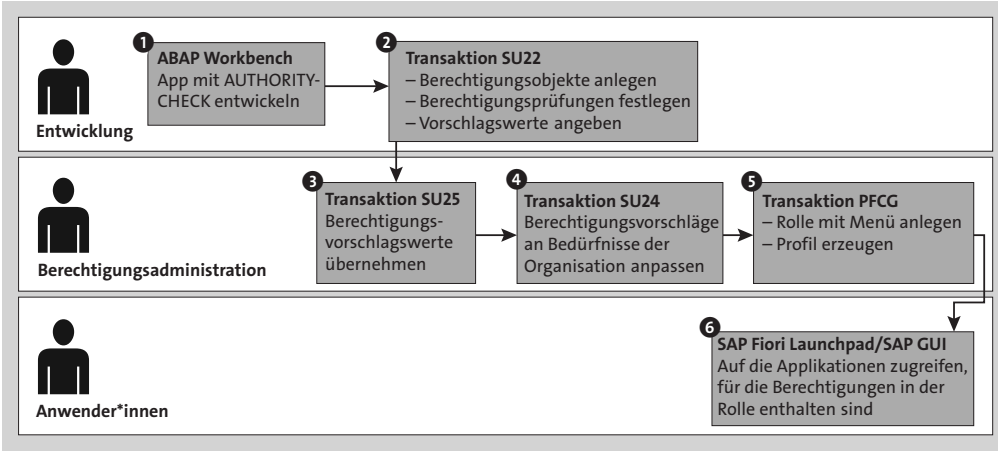


Abbildung 2.12 Ablauf der Tätigkeiten für die Berechtigungsprüfung

Berechtigungsvorschlagswerte für den Profilgenerator

Vorschlagswerte für Berechtigungen werden von SAP in Form der Tabellen USOBX und USOBT ausgeliefert. Mit den Inhalten dieser Tabellen werden die Kundentabellen USOBX_C und USOBT_C initial gefüllt. Das ist die Vor-

aussetzung für die richtige Funktion des Profilgenerators (Transaktion PFCG) bei der Anlage der Rollen.

Nach jedem Upgrade müssen die aktualisierten Daten aus den SAP-Tabellen in die Kundentabellen übernommen werden (siehe Abbildung 2.13).

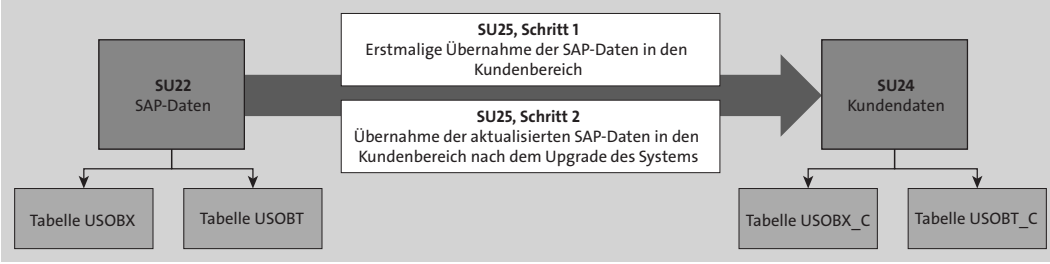


Abbildung 2.13 Übernehmen der SAP-Vorschlagswerte in die Kundentabellen

Tabellen USOBX, USOBT, USOBX_C, USOBT_C

Die Tabellen USOBT und USOBT_C definieren pro Transaktion und App Berechtigungsobjekte und Vorschlagswerte in den Feldern der Berechtigungsobjekte. Die Tabellen USOBX und USOBX_C enthalten Prüfkennzeichen für Berechtigungsobjekte. Nur die Berechtigungsprüfungen, die mit dem Kennzeichen Prüfen mit Vorschlag »Ja« versehen werden, gelangen als Vorschlagswerte in die Rolle.

Prüfkennzeichen in der Transaktion SU24

In Tabelle 2.2 sehen Sie die möglichen Prüfkennzeichen in den Transaktionen SU25 und SU24 und den Tabellen USOBX und USOBX_C.

Prüfkennzeichen	Vorschlagsstatus	Erläuterung
Prüfen	Ja	Das Objekt wird zusammen mit den gepflegten Feldwerten automatisch vom Profilgenerator aufgenommen.
Prüfen	Ja, ohne Werte	Das Objekt wird vom Profilgenerator automatisch aufgenommen. Sämtliche Berechtigungsfelder müssen von der Berechtigungsadministration mit kundenspezifischen Werten gepflegt werden.
Prüfen	Ja, inaktiver Vorschlag	Objekte mit diesem Prüfkennzeichen dürfen sowohl mit als auch ohne Feldwerte ausgeliefert werden. In der Rollenpflege bleibt ein inaktiver Vorschlag unberücksichtigt.

Tabelle 2.2 Prüfkennzeichen in der Transaktion SU24

Prüfkennzeichen	Vorschlagsstatus	Erläuterung
Prüfen	Nein	Diesen Status erhalten alle Objekte, die zur Ausführung von Funktionen innerhalb der App nicht benötigt werden, weshalb kein Berechtigungsvorschlag in die Rollen aufgenommen wird.
Nicht prüfen	Nein	Dieses Prüfkennzeichen wird gesetzt, wenn die eigene App eine externe Funktion erfolgreich ausführen soll, ohne für die erforderlichen Objekte Berechtigungsvorschläge erzeugen zu müssen.

Tabelle 2.2 Prüfkennzeichen in der Transaktion SU24 (Forts.)

In Abbildung 2.14 sehen Sie ein Beispiel der Prüfkennzeichen für die Transaktion PFCG in der Transaktion SU24.

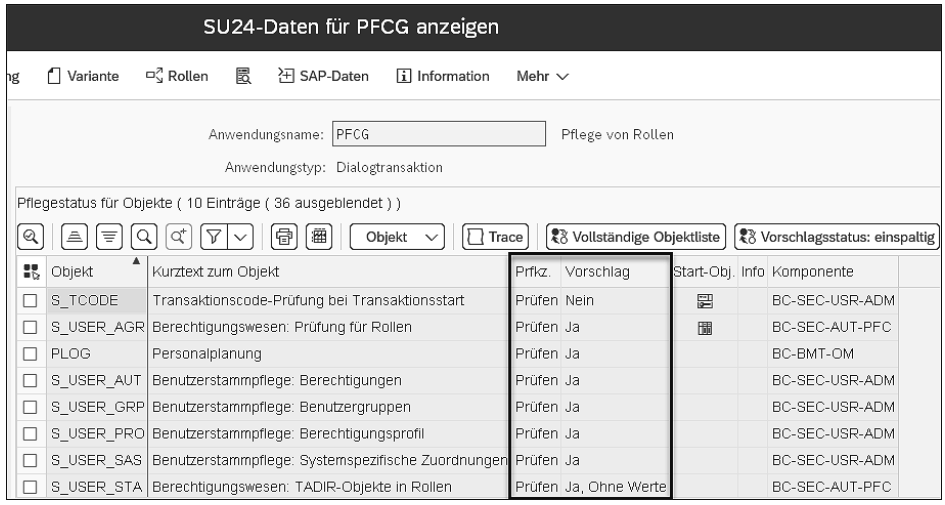


Abbildung 2.14 Beispiel für Prüfkennzeichen in den SU24-Daten für die Transaktion PFCG

2.3.2 Ausschalten der Berechtigungsprüfungen

Sie haben die Möglichkeit, den Umfang der Berechtigungsprüfungen über die Transaktion SU24 zu reduzieren. Beim Ausführen der Transaktionen im SAP-System wird häufig eine große Zahl von Berechtigungsobjekten geprüft, da im Hintergrund andere Transaktionen aufgerufen werden. Für eine erfolgreiche Prüfung müssen Benutzer über die entsprechenden Berechti-

gungen verfügen. Dadurch erhalten manche Benutzer mehr Berechtigungen als unmittelbar nötig. Außerdem bedeutet dies einen erhöhten Pflegeaufwand. Erwägen Sie zur Erleichterung der Verwaltungsaufgaben mit dem Profilgenerator, den Umfang der Berechtigungsprüfungen zu reduzieren.

Notwendigkeit einer Programmänderung

Für das Unterbinden von Berechtigungsprüfungen sind keine Programmänderungen erforderlich, da die Prüfungen über die Prüfkennzeichen gesteuert werden. Andersherum funktioniert es leider nicht: Sie können über die Transaktion SU24 und die Prüfkennzeichen keine zusätzlichen Berechtigungsprüfungen nachträglich für Transaktionen und Apps implementieren. Dafür ist eine Programmänderung notwendig.

Berechtigungsobjekte, die nicht von einer Prüfung ausgenommen werden können

Berechtigungsobjekte aus den Bereichen Basis (S_*) und Personalwirtschaft (P_*, PLOG) können Sie nicht von einer Prüfung ausnehmen.

Bei Parameter- oder Variantentransaktionen können Sie Berechtigungsobjekte nicht direkt, sondern nur über die Berechtigungsobjekte der eigentlichen Transaktion von einer Prüfung ausnehmen.

Risiko des Ausschaltens der Berechtigungsprüfung

Überlegen Sie genau, welche Berechtigungsprüfungen Sie unterdrücken möchten. Wenn Sie Berechtigungsprüfungen unterdrücken, gestatten Sie den Benutzern, Aufgaben durchzuführen, für die sie nicht ausdrücklich berechtigt sind.

Deaktivierte Berechtigungsprüfungen suchen

In Tabelle USOBX_C finden Sie Berechtigungsprüfungen, die im System durch die Pflege der Berechtigungsvorschlagswerte (Transaktion SU24) deaktiviert wurden. Suchen Sie dafür in der Tabelle USOBX_C über die Transaktion SE16 Einträge, bei denen das Feld OKFLAG auf »N« gesetzt ist.

Globales Ausschalten der Berechtigungsobjekte

Sie können Berechtigungsprüfungen für einzelne Berechtigungsobjekte über die Transaktion AUTH_SWITCH_OBJECTS global unterdrücken. Falls Sie diese Option verwenden, führt das System für die angegebenen Objekte keinerlei Berechtigungsprüfungen durch. Bei Verwendung des Profilgenerators verringert die Option den Aufwand für die Berechtigungspflege. Der Profilgenerator trägt für deaktivierte Berechtigungsobjekte keine Berechtigungsdaten in die Profile ein. Außerdem müssen Sie die Berechtigungsdaten im Anschluss an ein Upgrade für Transaktionen, deren entsprechende Berechtigungsobjekte Sie global deaktiviert hatten, nicht nachbearbeiten.

Berechtigungsobjekte, die global nicht ausgeschaltet werden können

Berechtigungsprüfungen von Berechtigungsobjekten, die zu Komponenten der Basis oder der Human Resources (HR) gehören, können Sie nicht global ausschalten.

2.3.3 SAP-Standardtabellen zur Steuerung der Benutzer- und Berechtigungsverwaltung

Tabellen PRGN_ CUST, SSM_CUST, USR_CUST

Die in Tabelle 2.3 aufgeführten SAP-Standardtabellen sind Customizing-Tabellen, die zentral für die Steuerung des Benutzer- und Berechtigungsmanagements verwendet werden.

Tabelle	Beschreibung
PRGN_CUST	Customizing-Einstellungen zum Berechtigungswesen
SSM_CUST	Einstellung von Werten für den Session Manager/Profilgenerator
USR_CUST	Customizing-Einstellungen zu Benutzern /Berechtigungswesen

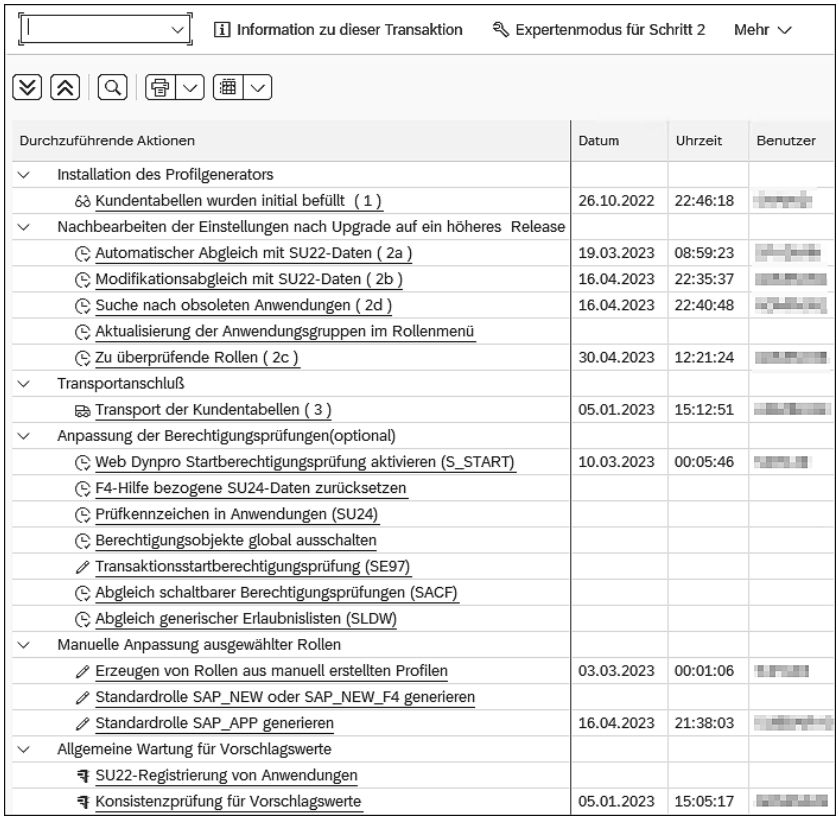
Tabelle 2.3 Customizing-Tabellen für die Steuerung des Benutzer- und Berechtigungsmanagements

2.4 Post-Upgrade-Tätigkeiten in der Transaktion SU25

Ein neues Release bringt neue technische Funktionen sowie neue Berechtigungsobjekte und -werte mit sich. Damit die neuen Berechtigungen nicht nur in Ihrem System verfügbar, sondern auch im Kontext Ihrer Anwendungen und in Ihren Rollen integriert werden, ist es erforderlich, die Post-Upgrade-Tätigkeiten in der Transaktion SU25 durchzuführen. In diesem Abschnitt erhalten Sie eine Beschreibung der Tätigkeiten in der Transaktion SU25 unter dem Knoten **Nachbearbeiten der Einstellungen nach Upgrade auf ein höheres Release**.

In Abschnitt 11.1, »Arbeitsschritte im SU25-Abgleich«, finden Sie eine detaillierte Aufführung aller Aktivitäten, einschließlich einer bildbasierten Schritt-für-Schritt-Hilfestellung zur Durchführung der Aktivitäten.

Die Ansicht der Transaktion SU25 und die darin relevanten Schritte für die Post-Upgrade-Tätigkeiten sehen Sie in Abbildung 2.15 unter dem Knoten **Nachbearbeiten der Einstellungen nach Upgrade auf ein höheres Release**. Im rechten Bereich sehen Sie den Zeitstempel der letzten Ausführung sowie den Benutzer, der die Ausführung vorgenommen hat.



Durchzuführende Aktionen	Datum	Uhrzeit	Benutzer
Installation des Profilgenerators			
Kundentabellen wurden initial befüllt (1)	26.10.2022	22:46:18	
Nachbearbeiten der Einstellungen nach Upgrade auf ein höheres Release			
Automatischer Abgleich mit SU22-Daten (2a)	19.03.2023	08:59:23	
Modifikationsabgleich mit SU22-Daten (2b)	16.04.2023	22:35:37	
Suche nach obsoleten Anwendungen (2d)	16.04.2023	22:40:48	
Aktualisierung der Anwendungsgruppen im Rollenmenü			
Zu überprüfende Rollen (2c)	30.04.2023	12:21:24	
Transportanschluß			
Transport der Kundentabellen (3)	05.01.2023	15:12:51	
Anpassung der Berechtigungsprüfungen(optional)			
Web Dynpro Startberechtigungsprüfung aktivieren (S_START)	10.03.2023	00:05:46	
F4-Hilfe bezogene SU24-Daten zurücksetzen			
Prüfkennzeichen in Anwendungen (SU24)			
Berechtigungsobjekte global ausschalten			
Transaktionsstartberechtigungsprüfung (SE97)			
Abgleich schaltbarer Berechtigungsprüfungen (SACF)			
Abgleich generischer Erlaubnislisten (SLDW)			
Manuelle Anpassung ausgewählter Rollen			
Erzeugen von Rollen aus manuell erstellten Profilen	03.03.2023	00:01:06	
Standardrolle SAP_NEW oder SAP_NEW_F4 generieren			
Standardrolle SAP_APP generieren	16.04.2023	21:38:03	
Allgemeine Wartung für Vorschlagswerte			
SU22-Registrierung von Anwendungen			
Konsistenzprüfung für Vorschlagswerte	05.01.2023	15:05:17	

Abbildung 2.15 Startansicht der Transaktion SU25

2.4.1 Installation des Profilgenerators – Kundentabellen werden initial befüllt (Schritt 1)

Die Installation des Profilgenerators ist ausschließlich und einmalig bei der Neuinstallation eines Systems durchzuführen. Nach einem Releasewechsel sollten Sie diesen Schritt nicht mehr ausführen. Bei den Tabellen USOBX und USOBT handelt es sich um die relevanten SAP-Tabellen, die die Datengrundlage für die Transaktion SU22 bilden. Die SAP-Tabellen für die Transaktion SU24 sind die Tabellen USOBX_C und USOBT_C (_C steht für Customer).

Initial sind die Transaktion SU24 und somit die Tabellen USOBX_C und USOBT_C leer. Mit Schritt 1 werden die Vorschlagswerte und Prüfkennzeichen aus den Tabellen USOBX und USOBT in die Tabellen USOBX_C und USOBT_C kopiert. Dieser Vorgang ist in Abbildung 2.16 dargestellt.

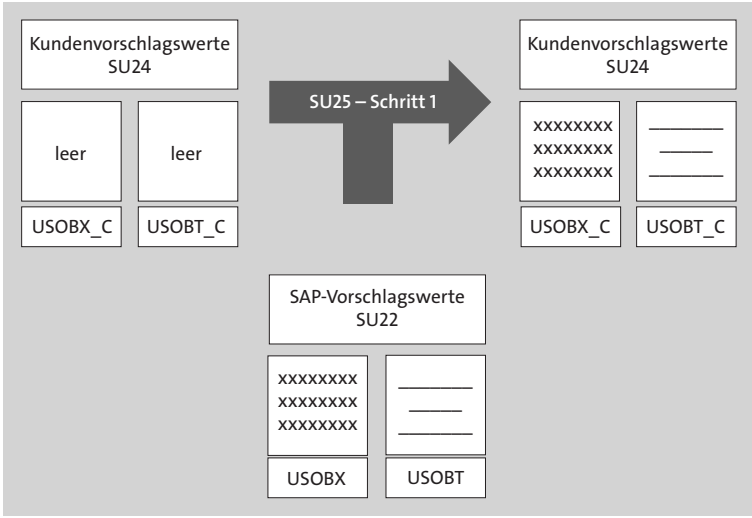


Abbildung 2.16 Transaktion SU25: der technische Ablauf in Schritt 1

Im Laufe der Zeit passen Sie Ihre SU24-Vorschlagswerte gemäß Ihren Anforderungen an und behalten diese bei. Mit erneuter Durchführung von Schritt 1 würden Sie Ihre SU24-Daten mit den SU22-Daten überschreiben. Ihre bis dahin angepassten SU24-Vorschlagswerte würden dann verloren gehen.

Reports SU2X_CHECK_CONSISTENCY und SU24_AUTO_REPAIR

Sie beginnen die Post-Upgrade-Aktivitäten mit der Konsistenzprüfung der SU24-Daten mit dem Report SU2X_CHECK_CONSISTENCY (eine Praxisübung hierzu finden Sie in Abschnitt 11.1.5) und der anschließenden Bereinigung von Inkonsistenzen mit dem Report SU24_AUTO_REPAIR (eine Praxisübung hierzu finden Sie in Abschnitt 11.1.6).

2.4.2 Automatischer Abgleich mit SU22-Daten (Schritt 2a)

Nicht veränderte Anwendungen in der Transaktion SU24

Anwendungen, die von Kunden in der Transaktion SU24 bisher nicht angepasst wurden, werden in diesem Schritt automatisch mit den SU22-Daten abgeglichen und aktualisiert. In Abbildung 2.17 sehen Sie eine Darstellung dieses Vorgangs. Die Transaktion ABC wurde vom Kunden bisher in der Transaktion SU24 nicht verändert.

Im alten Release wurden im Kontext der Transaktion ABC die Berechtigungsobjekte 1 und 2, einschließlich der Berechtigungsfelder 1 und 2, mit den Berechtigungswerten 1 und 2 geprüft und vorgeschlagen. Im neuen Release kommen nach dem automatischen Abgleich in Schritt 2a noch ein Berechtigungswert in Berechtigungsobjekt 1 sowie ein drittes Berechtigungsobjekt automatisch hinzu. Eine detaillierte Anleitung zum automa-

tischen Abgleich der SU22-Daten finden Sie in Abschnitt 11.1.7, »Post-Upgrade: Praxisübung zu Schritt 2a«.

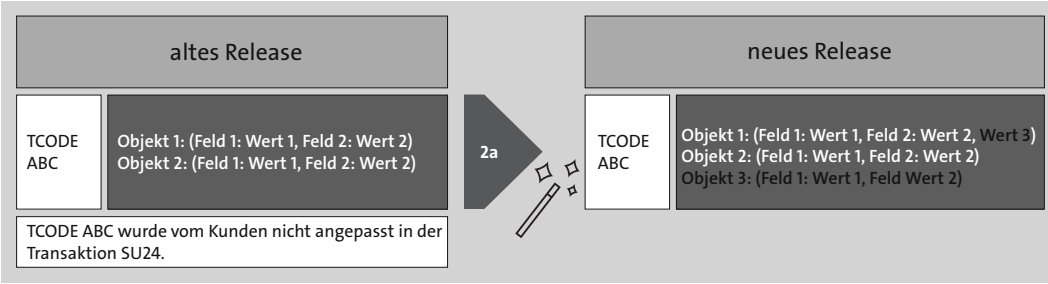


Abbildung 2.17 Transaktion SU25: automatischer Abgleich der SU24-Vorschlagswerte

2.4.3 Modifikationsabgleich mit SU22-Daten (Schritt 2b)

Veränderte Anwendungen in der Transaktion SU24

Im Laufe der Zeit nehmen Sie im Rahmen Ihrer Berechtigungsverwaltung Veränderungen der SU24-Vorschlagswerte im alten Release vor. Die Veränderung kann im Hinzufügen und Entfernen von Berechtigungsobjekten bestehen oder in der Anpassung der Prüfkennzeichen sowie in der Bearbeitung der Berechtigungswerte.

Das hat zur Folge, dass die veränderten Anwendungen aus Schritt 1 nicht mehr automatisch abgeglichen werden, sondern manuell in Schritt 2b abgeglichen werden müssen (siehe Abbildung 2.18). Für jede dieser Transaktionen gleichen Sie Ihre SU24-Vorschlagswerte mit den SAP-Vorschlagswerten ab und entscheiden, ob Sie Ihre Daten beibehalten oder die von SAP übernehmen möchten.

In Abschnitt 11.1.8, »Post-Upgrade: Praxisübung zu Transaktion SU25 Schritt 2b«, finden Sie eine detaillierte Anleitung für den Modifikationsabgleich der SU22-Daten.

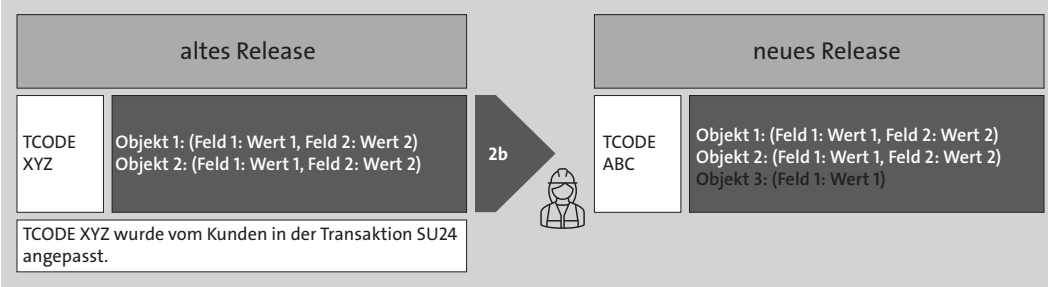


Abbildung 2.18 Transaktion SU25: manueller Abgleich der SU24-Vorschlagswerte

2.4.4 Zu überprüfende Rollen (Schritt 2c)

Umgang mit betroffenen Rollen

In diesem Schritt werden die Rollen, deren Menüanwendungen von den Änderungen der SU24-Vorschlagswerte betroffen sind, abgemischt, sodass die aktualisierten Werte in die Rollen gelangen. Nach einem Klick auf **Zu überprüfende Rollen (2c)** erhalten Sie zunächst einen Hinweistext. Anschließend werden die betroffenen Rollen aufgeführt, die Sie dann nacheinander prüfen und abmischen können. Wie bei Rollen üblich, sind die Anpassungen mandantenspezifisch. Beachten Sie außerdem:

- Die Dauer bis zur Anzeige der Ergebnisliste hängt von der Gesamtzahl der im aktuellen Mandanten existierenden Rollen ab. Bei mehreren Tausend zu untersuchenden Rollen ist mit Laufzeiten im Minutenbereich zu rechnen.
- Die Navigation von der Ergebnisliste in die Berechtigungsdaten erfolgt entweder durch einfachen Klick auf den gewünschten Rollennamen oder per Doppelklick auf eine beliebige andere Stelle derselben Zeile.
- Schritt 2c berücksichtigt nur Rollen im aktuellen Mandanten. Falls Sie Rollenentwicklung in mehreren Mandanten betreiben, müssen Sie den Schritt in jedem dieser Mandanten ausführen.

In Abschnitt 11.1.10, »Post-Upgrade: Praxisübung zu Transaktion SU25 Schritt 2c«, finden Sie eine detaillierte Anleitung zu Schritt 2c.

2.4.5 Suche nach obsoleten Anwendungen (2d)

Berücksichtigung von neuen Transaktionen

Es kommt vor, dass Transaktionen im SAP-System gelöscht oder durch andere Transaktionen ersetzt werden. In **Suche nach obsoleten Anwendungen (2d)** erhalten Sie nach der Ausführung eine Liste von Rollen, die obsolete Transaktionen im Rollenmenü enthalten. Eine Transaktion kann obsolet sein, wenn sie nicht mehr existiert bzw. veraltet ist und nicht mehr verwendet wird. Es kann aber auch sein, dass SAP eine Sperre für diese Anwendungen gesetzt hat oder der Status dieser Anwendungen in der Transaktion SU22 veraltet ist. Es passiert auch häufig, dass eine Transaktion durch eine oder mehrere Transaktionen ersetzt wird. Dieser Schritt ist in Abstimmung mit den Prozess- bzw. Rollenverantwortlichen auf Anwenderseite durchzuführen. In Abschnitt 11.1.10 finden Sie eine Praxisübung zu diesem Schritt.

Backup der SU24-Daten

Beachten Sie bitte, dass Sie, bevor Sie die SU25-Upgrade-Aktivitäten durchführen, den aktuellen Stand Ihrer Transaktion SU24 als Backup sichern. Das

Backup erstellen Sie mithilfe von Schritt 3 in der Transaktion SU25. Nach der Ausführung von Schritt 3 halten Sie den aktuellen Stand der Tabellen USOBX_C und USOBT_C in einem Transportauftrag fest. Der freigegebene Transportauftrag dient Ihnen als Backup und kann im Bedarfsfall von der SAP-Basisadministration wieder ins Entwicklungssystem importiert werden.

2.5 CDS-Views

Seit der Verfügbarkeit der SAP-HANA-Plattform hat sich bei SAP ein Paradigmenwechsel in der Entwicklung von Geschäftsanwendungen vollzogen. Die Faustregel lautet: Entwickeln Sie so viel wie möglich in der Datenbank, um die beste Leistung zu erzielen.

Core Data Services

Um die Vorteile von SAP HANA für die Anwendungsentwicklung zu nutzen, hat SAP eine neue Datenmodellierungsinfrastruktur eingeführt, die als *Core Data Services* (CDS) bekannt ist.

Mit CDS werden Datenmodelle in der Datenbank und nicht auf dem Anwendungsserver definiert und genutzt. CDS bietet auch Funktionen, die über die herkömmlichen Datenmodellierungstools hinausgehen, einschließlich der Unterstützung für die konzeptionelle Modellierung und Beziehungsdefinitionen, integrierte Funktionen und Erweiterungen. CDS-Views sind eine Infrastruktur zum Definieren und Nutzen von semantisch umfangreichen Datenmodellen in SAP HANA.

Bei CDS-Views wird zwischen *SAP-HANA-CDS-Views* und *ABAP-CDS-Views* unterschieden.

SAP-HANA-CDS-Views

SAP-HANA-CDS-Views werden auf SAP-HANA-Datenbankebene definiert. Sie werden in *DDL*-Dateien (*Data Definition Language*) erstellt und verwaltet, die in *SAP HANA XS* (*HANA Extended Application Services*) gespeichert sind. Die Views verwenden Native SQL als Programmiersprache. HANA-CDS-Views zielen darauf ab, die Entwicklung nativer SAP-HANA-Anwendungen zu unterstützen. Sie nutzen Funktionen, die nur für SAP HANA verfügbar sind. Sie können nur mit einer HANA-Datenbank verwendet werden. Der Hauptfokus von HANA-CDS-Views liegt auf der Erstellung von Modellen direkt in der Datenbank.

ABAP-CDS-Views

ABAP-CDS-Views werden auf Anwendungsserverebene definiert. Sie werden in DDL-Dateien auf dem ABAP-Anwendungsserver erstellt und verwaltet. Sie befinden sich im ABAP Data Dictionary in der Transaktion SE11 und werden mit dem SAP-Transportsystem transportiert. ABAP-CDS-Views ver-

wenden Open SQL als Programmiersprache. Ihr Ziel ist es, die Entwicklung von ABAP-Anwendungen zu unterstützen. Die Art der Datenbank spielt keine Rolle, es muss nicht unbedingt SAP HANA sein. Der Hauptfokus von ABAP-CDS-Views liegt auf der Erstellung von Views.

ABAP-CDS-Views wurden mit dem Release ABAP 7.40 SP08 eingeführt, damit die neue Technologie unabhängig von der Art der Datenbank auf einem SAP-System verwendet werden kann.

In Tabelle 2.4 sind die Hauptunterschiede zwischen ABAP-CDS-Views und SAP-HANA-CDS-Views dargestellt.

	ABAP-CDS-Views	SAP-HANA-CDS-Views
Residenz	Applikationsserver	SAP HANA XS
Datenbank	alle Datenbanken	Nur SAP HANA DB
Programmiersprache	Open SQL	Native SQL
Ziel	ABAP-Anwendungen	Native HANA-Anwendungen
Hauptfokus	Views erstellen	Modelle erstellen

Tabelle 2.4 Hauptunterschiede zwischen ABAP-CDS-Views und SAP-HANA-CDS-Views

Vorteile von CDS-Views

CDS-Views sind eine Kerntechnologie von SAP S/4HANA und erweitern die Möglichkeiten der Datenmodellierung. Aus der Nutzung von CDS-Views ergeben sich für Organisationen folgende Vorteile:

- **Performance-Steigerung**
  Da die Rechenoperationen in einem CDS-View auf die HANA-Datenbank verschoben werden, wird die Bearbeitungsstärke auf die In-Memory-Datenbank verlagert. Dies führt zu einer großen Performance-Steigerung.
- **Größere Datenmodellierungsmöglichkeiten**
  CDS-Views haben den Vorteil, dass sie programmierbar sind. Dies bedeutet, dass Sie viele unterschiedliche Möglichkeiten bei der Datenmodellierung bieten.
- **Zeitersparnis bei der Fiori-App-Entwicklung**
  CDS-Views können bei der Entwicklung neuer Fiori-Apps verwendet werden.

- **Datenmodellerweiterungen für SAP S/4HANA**
  Da es sich um virtuelle Objekte/Programmiermodelle handelt und somit das Datenmodell per Laufzeit erzeugt wird, können dem Datenmodell weitere Felder oder zusätzliche Information ohne größeren Aufwand hinzugefügt werden.

Das Berechtigungskonzept für CDS-Views

Für CDS-Views gibt es ein eigenes Berechtigungskonzept, das auf einer Datenkontrollsprache (*Data Control Language*, *DCL*) basiert. Das Berechtigungskonzept für CDS verwendet definierte Bedingungen und greift auf klassische Berechtigungen (PFCG-Rollen und Berechtigungsobjekte) zurück.

Unterschied zwischen ABAP- und CDS-Berechtigungen

Neben dem CDS-Berechtigungskonzept existiert noch das klassische Berechtigungskonzept von SAP NetWeaver Application Server für ABAP (siehe Abschnitt 1.4., »Berechtigungen in SAP ECC«). Das klassische Berechtigungskonzept basiert auf Berechtigungsobjekten. Die Berechtigung eines Benutzers erfolgt entweder implizit, z. B. beim Aufrufen einer Transaktion, oder explizit mit der Anweisung `AUTHORITY-CHECK`. Das CDS-Berechtigungskonzept basiert auf impliziten Berechtigungsprüfungen, die bei Zugriffsversuchen auf CDS-Entitäten durchgeführt werden.

CDS-Zugriffskontrollen

CDS-Zugriffskontrollen basieren auf CDS-Rollen, die in DCL definiert sind. Beim Zugriff auf CDS-Entitäten, die einer CDS-Rolle zugeordnet sind, werden zusätzliche Zugriffsbedingungen ausgewertet. Im Fall einer analytischen Abfrage (basierend auf einer CDS-Entität mit Zugriffskontrollen) bedeutet das, dass zur Laufzeit der Abfrage die berechtigten Werte der SQL-Anweisung mit einem logischen `UND` zur `WHERE`-Klausel hinzugefügt werden. Zugriffskontrollen werden nur ausgewertet, wenn ein Open-SQL-Zugriff auf die Entität besteht, für die die Zugriffskontrolle definiert ist (`grant select on` (siehe beispielhaft in Abbildung 2.19)).

Berechtigte Werte werden automatisch als Filterwerte angewendet. Bei fehlenden Berechtigungen erhält ein Benutzer daher keine Fehlermeldung wie »Keine Berechtigung ...«, sondern es werden keine oder weniger Daten in der Abfrage angezeigt.

```
@EndUserText.label: 'Auto assigned mapping role for I_ActualPlanJrnlEntryItemCube'
@MappingRole: true
define role I_ActualPlanJrnlEntryItemCube {
    grant select on I_ActualPlanJrnlEntryItemCube inherit I_ActualPlanJournalEntryItem;



//    where
//         ( Ledger )       = aspect pfcg_auth ( F_FAGL_LDR, GLRLDNR, actvt = '03' )
//     AND ( CompanyCode )  = aspect pfcg_auth ( F_BKPF_BUK, BUKRS  , ACTVT = '03' )
//     AND ( BusinessArea ) = aspect pfcg_auth ( F_BKPF_GSB, GSBER  , ACTVT = '03' )
//     AND ( Segment )      = aspect pfcg_auth ( F_FAGL_SEG, SEGMENT, ACTVT = '03' )
//     AND ( Ledger, CompanyCode, PlanningCategory, ControllingArea ) = aspect pfcg_auth ( K_ACDOCP_P, GLRLDNR, BUKRS, CATEGORY_P, KOKRS, ACTVT = '03' );
}
```

Abbildung 2.19 Beispiel für eine Zugriffskontrolle für CDS-View

Berechtigungsprüfung für SAP-Standard-CDS-Views

SAP liefert Standard-CDS-Views, die in Transaktionen und Fiori-Apps verwendet werden. Ob eine Transaktion oder Fiori-App CDS-Views und entsprechende Berechtigungsprüfungen verwendet, können Sie mithilfe eines Berechtigungstrace ermitteln (siehe Abschnitt 9.2.1, »Berechtigungsfehler lösen mit der Transaktion STAUTHTRACE«, und 9.3, »Fehlerbehebung für CDS-Views«).

Berechtigungsprüfung für kundeneigene CDS-Views

Wenn die Entwicklung kundeneigene Apps mit CDS-Views anlegt, muss sie die Berechtigungsprüfung für die Daten, gemäß den Anforderungen der Organisation, mit SAP-Standard- oder kundeneigenen Berechtigungsobjekten implementieren. Bei der Definition der Anforderungen an die Berechtigungsprüfung und ihrer Umsetzung empfehlen wir eine Zusammenarbeit von Entwicklung und Berechtigungsadministration.

2.6 Berechtigungstraces

Zweck von Berechtigungstraces

Mit dem System- oder Berechtigungstrace können Sie Berechtigungsprüfungen und deren Werte aufzeichnen. Diese Funktion unterstützt Sie beim Pflegen von Berechtigungsvorschlagswerten in der Transaktionen SU24 und bei der Pflege von Berechtigungsdaten in den Rollen in der Transaktion PFCG.

Die im SAP-System vorhandenen Traces werden in den folgenden drei Abschnitten vorgestellt.

2.6.1 Berechtigungstrace in der Transaktion STUSOBTRACE

Transaktion STUSOBTRACE

Mit der Transaktion STUSOBTRACE können Sie das Berechtigungstrace im SAP-System auswerten. Hierbei handelt es sich um ein Trace, das über einen längeren Zeitraum in mehreren Mandanten und benutzerunabhängig Berechtigungsdaten sammelt und in einer Datenbank (Tabelle USOB_AUTHVALTRC) ablegt. Sobald das Trace während der Ausführung eines Programms auf eine Berechtigungsprüfung stößt, die im Zusammenhang mit der aktuellen Anwendung bislang nicht erfasst war, legt es einen entsprechenden Eintrag in der Trace-Datenbanktabelle an. Testen Sie die Anwendung möglichst vollständig, um aussagekräftige Trace-Daten zu erhalten (siehe Abbildung 2.20).

Dieses Berechtigungstrace wird von SAP während der Entwicklung zur Ermittlung der in Transaktion SU22 verwendeten Berechtigungsvorschlagswerte für Transaktionen, RFC-Bausteine und Services benutzt.

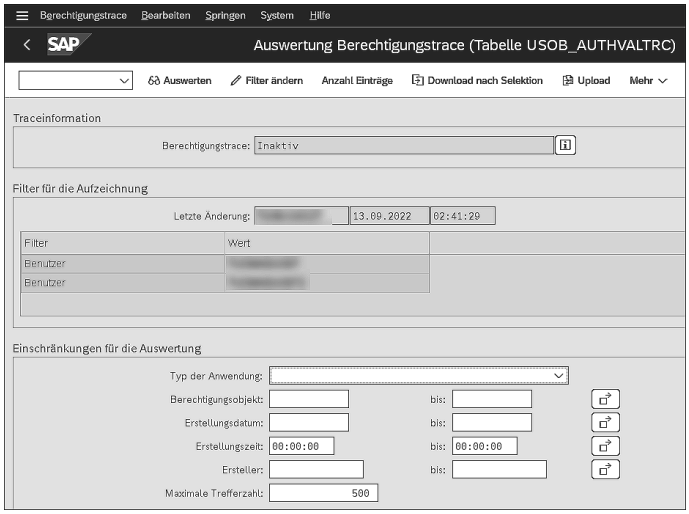


Abbildung 2.20 Berechtigungstrace in der Transaktion STUSOBTRACE

2.6.2 Systemtrace in den Transaktionen ST01 oder STAUTHTRACE

In den Transaktionen ST01 und STAUTHTRACE können Sie ein Kurzzeit-Trace, das Berechtigungsdaten mandantenabhängig und nur auf dem aktuellen Anwendungsserver sammelt, ausführen.

Transaktion STAUTHTRACE

In Transaktion STAUTHTRACE können Sie die Auswertung direkt filtern und eine bessere Auswertungsdarstellung erhalten. Über die einzelnen Buttons können Sie das Trace direkt ein- oder ausschalten und das Ergebnis des Trace anzeigen (siehe Abbildung 2.21).

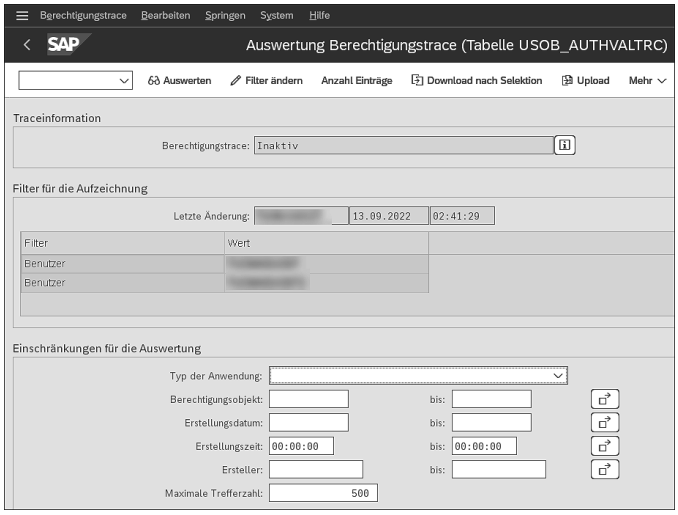


Abbildung 2.21 Systemtrace in der Transaktion STAUTHTRACE

Die Transaktion STAUTHTRACE wird in der Praxis am häufigsten von der Berechtigungsadministration zur Lösung von Berechtigungsfehlern verwendet.

Transaktion ST01

Zusätzlich können Sie das *Systemtrace* über die Transaktion ST01 aufrufen. Hierbei gibt es die Möglichkeit, einzelne Filter für die Prüfungen einzustellen (siehe Abbildung 2.22).

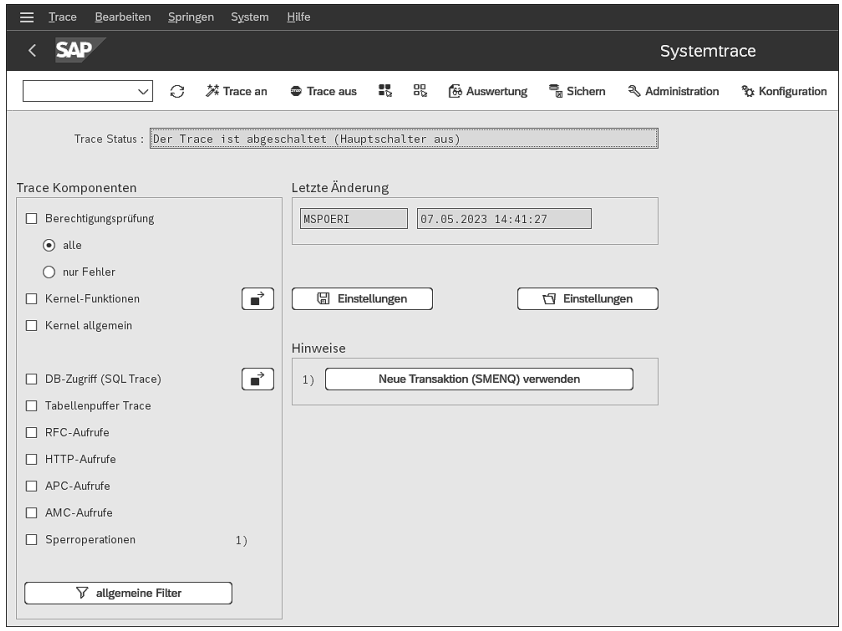


Abbildung 2.22 Systemtrace in der Transaktion ST01

2.6.3 Benutzertrace für Berechtigungsprüfungen in der Transaktion STUSERTRACE

Transaktion STUSERTRACE

In der Transaktion STUSERTRACE können Sie ein Langzeit-Trace, das mandanten- und benutzerbezogene Berechtigungsdaten sammelt und in der Datenbank ablegt, ausführen. Im Grunde genommen ist das das Berechtigungstrace in der Transaktion STUSOBTRACE, das nach einzelnen Benutzern filtert. Sie können die Transaktion STUSERTRACE aufrufen und den Filter auf einen einzelnen Benutzer einstellen (siehe Abbildung 2.23).

Ähnlich wie beim Berechtigungstrace aus Abschnitt 2.6.1, »Berechtigungstrace in der Transaktion STUSOBTRACE«, muss der Profilparameter `auth/auth_user_trace` in der Transaktion RZ10 oder RZ11 entsprechend gesetzt werden, damit Sie die Transaktion STUSERTRACE verwenden können.

Die Anleitungen zur Trace-Ausführung finden Sie in Abschnitt 9.2, »Traces in verschiedenen Szenarien anwenden«.

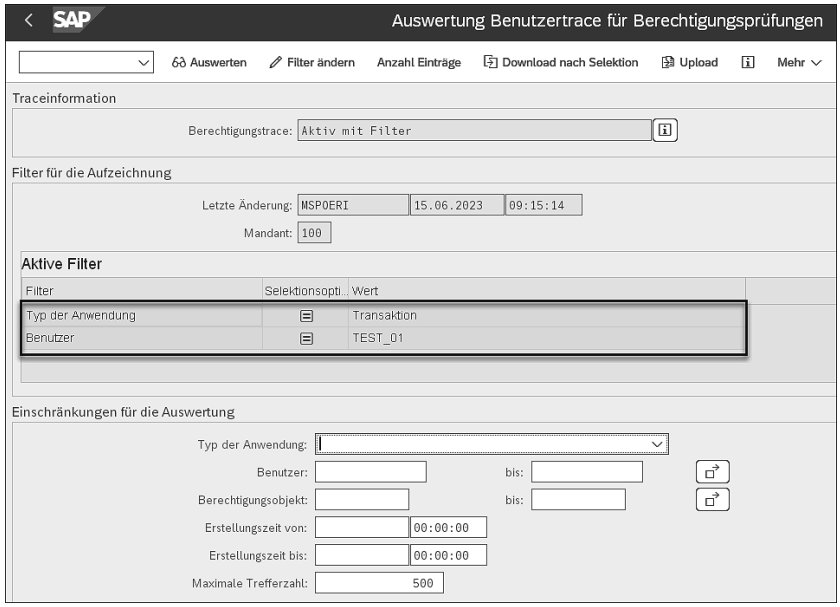


Abbildung 2.23 Benutzertrace für Berechtigungsprüfungen in der Transaktion STUSERTRACE

2.7 Zusammenfassung

In diesem Kapitel haben Sie einen tieferen Einblick in die Funktionsweisen der Berechtigungen in einem SAP-S/4HANA-System bekommen. Sie haben gelernt, aus welchen Komponenten eine PFCG-Rolle besteht, welche Rollenarten es gibt und wie sie zueinander stehen. Sie wissen nun, welche Menüobjekte es gibt und wie die Prüfung auf Berechtigungsobjekte und Feldwerte funktioniert.

Sie haben erfahren, aus welchen Komponenten der Benutzerstammsatz besteht, welche Benutzertypen es gibt und wie Single Sign-on für SAP Logon eingesetzt wird. Außerdem haben Sie gelernt, wie die Berechtigungsvorschlagswerte initial und nach dem System-Upgrade in der Transaktion SU25 in die Kundentabellen übernommen werden, wie Berechtigungsprüfungen für einzelne Transaktionen und Apps funktionieren und global ausgeschaltet werden können.

Sie wissen nun, welche Customizing-Tabellen es für die Benutzer- und Berechtigungsverwaltung und welche Transaktionen es für das Berechtigungstrace in einem SAP-System gibt. Darüber hinaus haben Sie in diesem Abschnitt die Arbeitsschritte, die zum SU25-Abgleich gehören, sowie die CDS-Views und die Berechtigungstraces kennengelernt.