Anleitung
SAP-Berechtigungen

Dieses Dokument dient der Wissensvermittlung von allgemeinem SAP-Know-how und erhebt keinen Anspruch auf Vollständigkeit oder Richtigkeit. Es basiert auf SAP-Dokumentationen, dem Wissen unserer Mitarbeiter und unseren Projekterfahrungen.

Falls Sie Fehler entdecken, Fragen haben oder Feedback geben möchten, senden Sie bitte eine Mitteilung an support@all-for-one.com. Vielen Dank.

All for One Switzerland AG | Bionstrasse 5 | CH-9015 St. Gallen
fon +41 (0) 58 255 74 00 | info.ch@all-for-one.com | www.all-for-one.ch
Ein Unternehmen der All for One Group SE

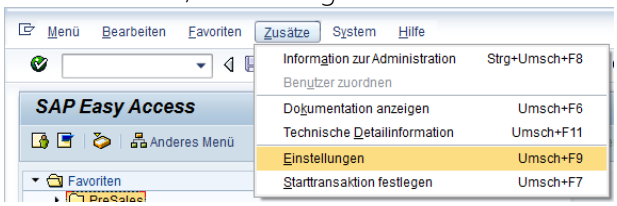
Inhaltsverzeichnis

1. SAP-Transaktion

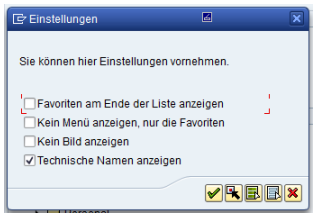
1.1 Wo finde ich den SAP-Transaktionscode

Im «SAP-Menü» und Benutzermenü können die Transaktionscodes eingeschaltet werden.

Menü **Zusätze** / Einstellungen



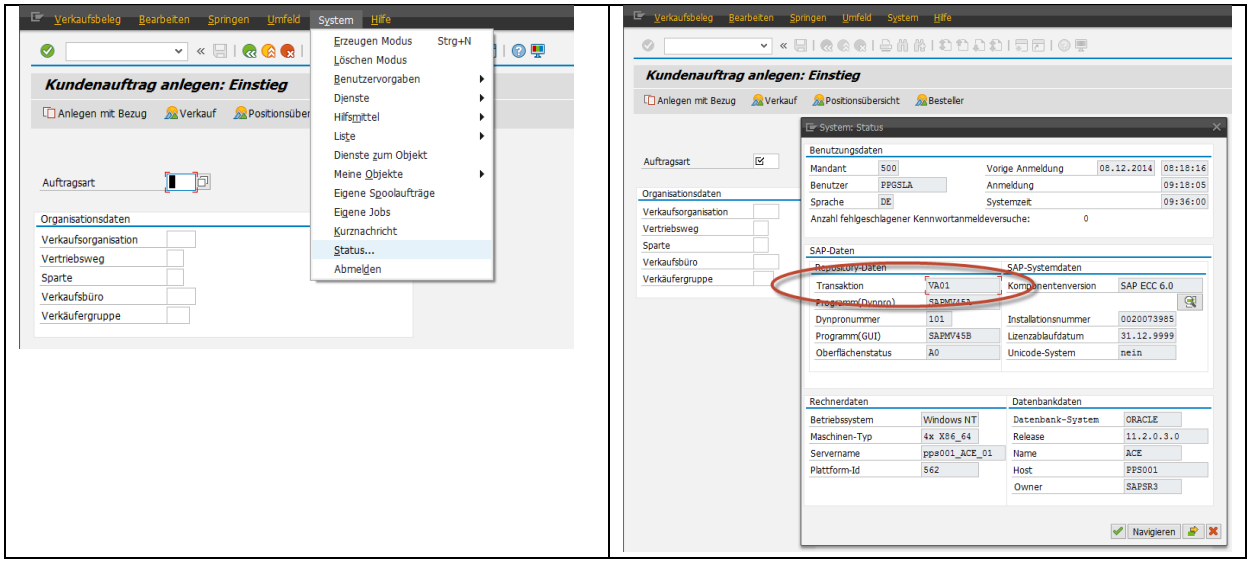
Ankreuzfeld «Technische Namen anzeigen» markieren und Enter-Taste (grüner Haken).



Anschliessend wird der Transaktionscode zu Beginn des Menüpunktes angezeigt.

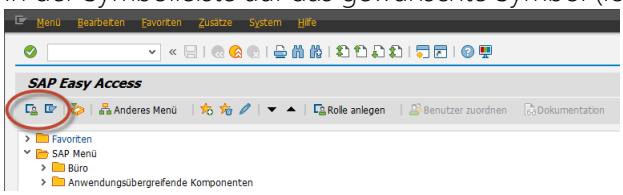
Alternativ, wenn ein Bildschirm angezeigt wird.

Menü System / Status . . .



1.2 Wechsel zwischen «SAP-Menü (Standard)» und Benutzermenü

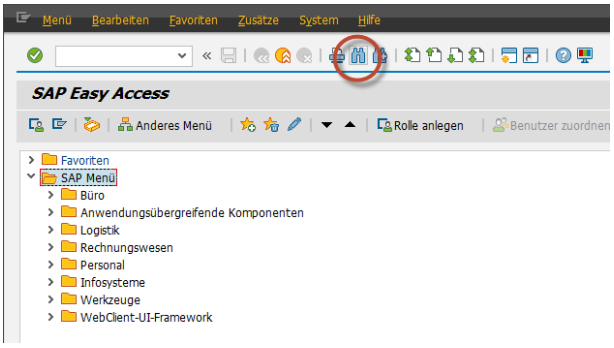
In der Symbolleiste auf das gewünschte Symbol (Icon) klicken



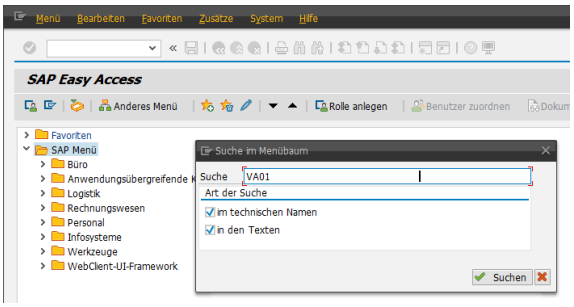
1.3 Wie finde ich den Transaktionscode xyz im «SAP-Menü» oder Benutzermenü

Suche im «SAP Menü» starten

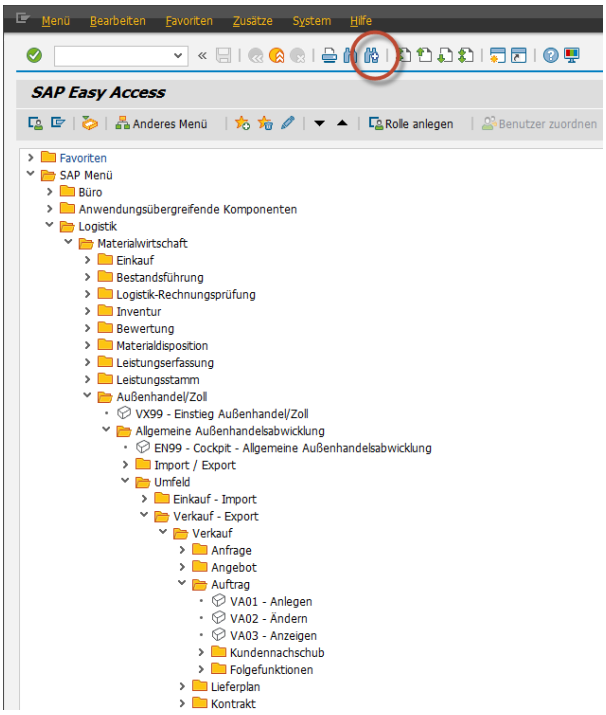
«**Feldstecher**» oder Tastenkombination **Ctrl+F**



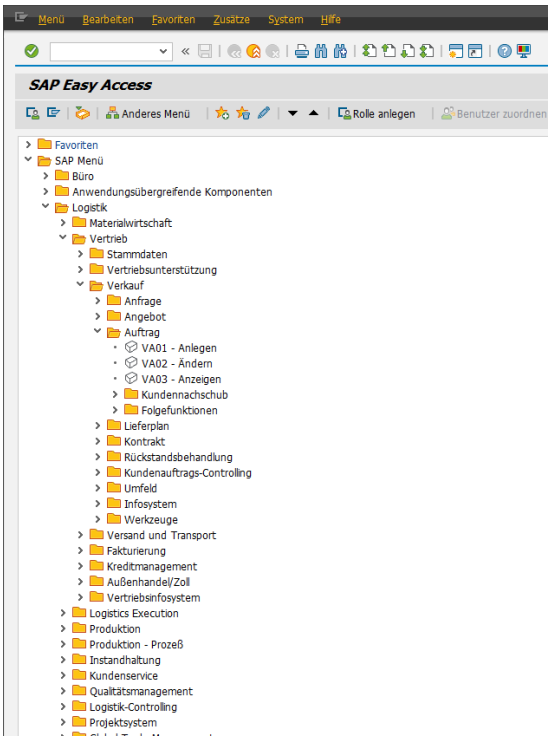
Suche nach «VA01»



Erstes Vorkommnis «VA01» ► weitersuchen



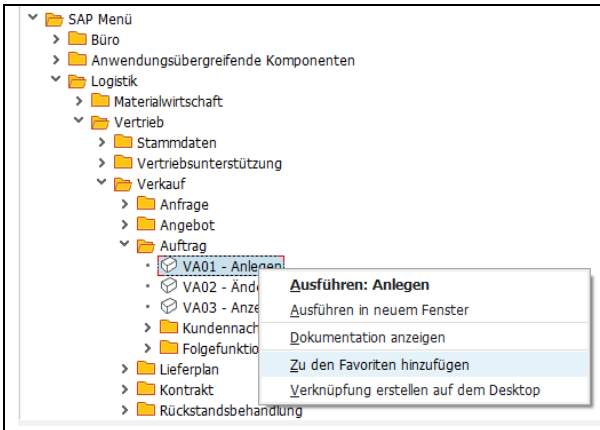
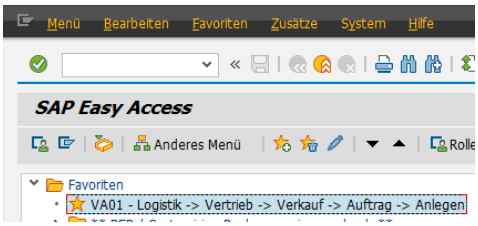
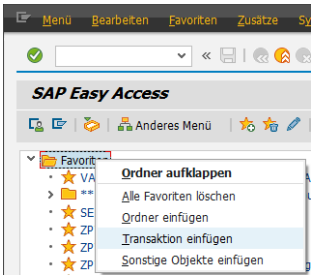
Ergebnis: gesuchter Eintrag



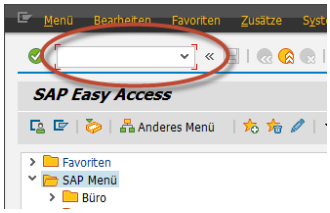
1.4 Aufruf einer Transaktion

Grundsätzlich kann eine Transaktion durch Doppelklick eines Menü-Eintrages aufgerufen werden. Wem das Suchen im Menü zu viel Arbeit ist, hat folgende weitere Möglichkeiten.

1.4.1 Aufruf einer Transaktion via Favoriten

<table>
<tr>
<td> 
</td>
<td>► Aufruf durch Doppelklick
 
</td>
</tr>
<tr>
<td>Transaktion manuell in Favoriten aufnehmen
► rechte Maustaste auf «Favoriten»
 
</td>
<td>Favoriten-Einträge können durch Doppelklick aufgerufen werden</td>
</tr>
</table>

1.4.2 Aufruf einer Transaktion via Befehlsfeld (Kommandofeld)



Sollte das Befehlsfeld nicht sichtbar sein ► Klick auf Doppel-Pfeil-Symbol und es sollte sich öffnen / schliessen

► weitere Infos ► im Feld positionieren und F1 Hilfe drücken

1.5 Transaktion SE93 Transaktionspflege

Diese Transaktion bietet z.B. folgende Funktionen.

- Transaktionen pflegen

2. Benutzerpflege

2.1. Transaktion SU01 Benutzerpflege

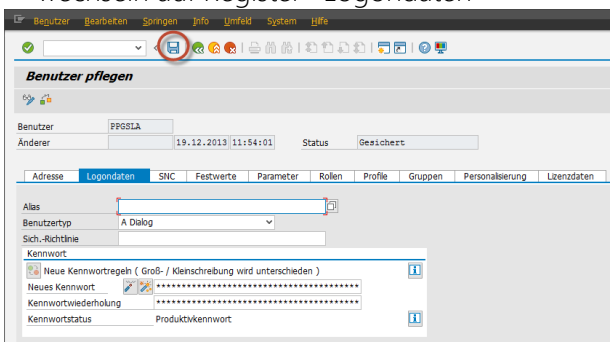
Diese Transaktion bietet z.B. folgende Funktionen.

- Benutzer anlegen/ändern/kopieren
- Rollen und Profile zuordnen
- Kennwort zurücksetzen
- Benutzer sperren / entsperren

2.1.1. Kennwort zurücksetzen

► aufrufen Transaktion «SU01 Benutzerpflege», Benutzer eingeben und Drucktaste «ändern»

► wechseln auf Register «Logondaten»



► neues Kennwort bei «Neues Kennwort» und «Kennwortwiederholung» eingeben und sichern

► bei der nächsten Anmeldung wird der Benutzer aufgefordert, dieses neue Kennwort zu ändern

2.1.2. Benutzer sperren / entsperren (z.B. zu viele Fehlversuche ► entsperren)

► aufrufen Transaktion «SU01 Benutzerpflege», Benutzer eingeben und Drucktaste «sperren / entsperren»

2.2. Transaktion SU10 Benutzerpflege Massenänderung

Diese Transaktion bietet für eine frei definierbare Menge von Benutzern z. B. folgende Funktionen.

- Benutzerstammdaten ändern
- Rollen- oder Profilzuordnungen ändern

3. Rollenverwaltung

3.1. Transaktion PFCG Rollenpflege

Diese Transaktion bietet z.B. folgende Funktionen.

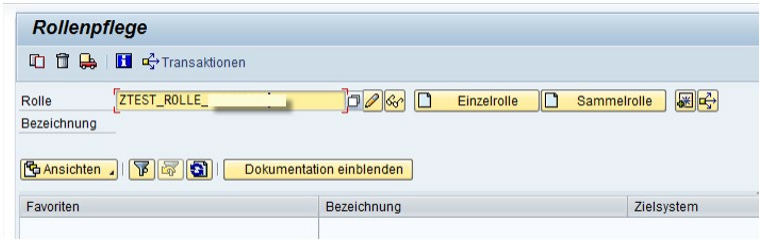
- Einzel- oder Sammelrollen pflegen (anlegen / ändern / löschen)
- Benutzerprofile generieren
- Rollenmenü pflegen (► erscheint im Benutzermenü)
- Rolle Benutzern zuordnen
- Benutzerabgleich durchführen
- Rollen transportieren

Nachfolgend der Grobablauf beim Anlegen einer neuen Rolle.

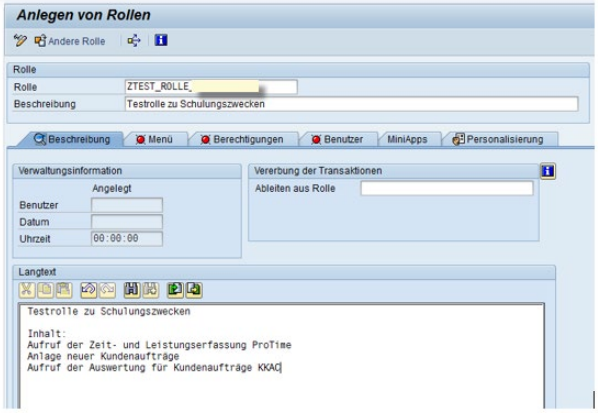
- Neue Rolle anlegen
- Definition einer Menüstruktur
- Zuordnung von Transaktionen
- Nachbearbeitung der Rolle im Profilgenerator
- Generierung der Rolle
- Zuordnung von Benutzern
- Durchführung eines Benutzerabgleichs

3.2. Rolle anlegen ► Schritte im Detail

► aufrufen der Transaktion PFCG Rollenpflege



► Rollenname (gemäss Namenskonvention) eingeben und Drucktaste **«Einzelrolle»** wählen

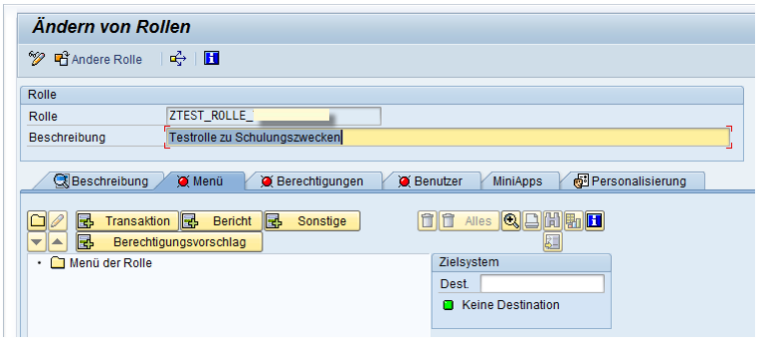


► im Feld «Beschreibung» eine Kurzbeschreibung eingeben sowie eine detaillierte Beschreibung im Langtext, um auch der «Nachwelt» einen schnellen Überblick über den Inhalt der Rolle zu geben.

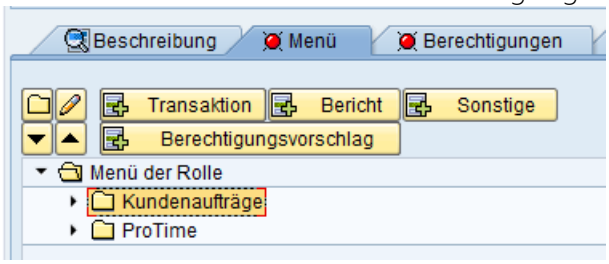
3.2.1. Menüstruktur definieren ► erscheint im Benutzermenü

Im Register **«Menü»** kann eine beliebige Ordnerstruktur innerhalb eines Rollenmenüs definiert werden.

3.2.1.1. Menüstruktur manuell pflegen

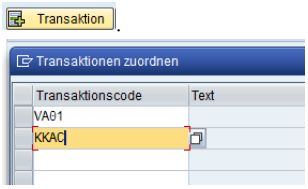


Mit der Drucktaste  können Ordner angelegt werden. Pflegen Sie eine beliebige Struktur.

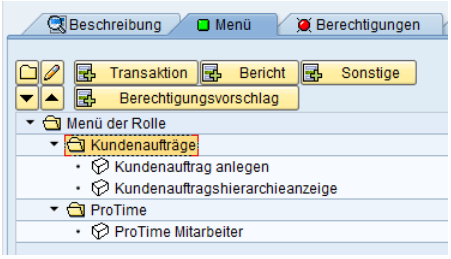


Mit den Drucktasten  können Sie die Reihenfolge der Ordner innerhalb der Struktur nach oben oder unten verschieben. Untergeordnete Ordner können via «Drag&Drop» innerhalb der Struktur verschoben werden.

Markieren Sie den Ordner, dem Sie Transaktionen hinzufügen möchten und wählen Sie die Drucktaste

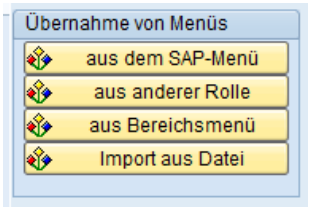


Gewünschte Transaktionen eingeben und mit Drucktaste Transaktionen zuordnen bestätigen. Die Transaktionen werden in der Struktur hinzugefügt.

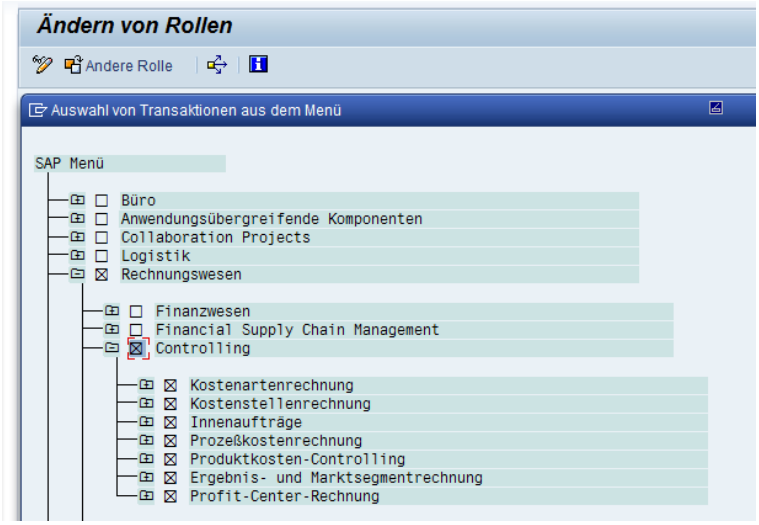


3.2.1.2. Menüstruktur ableiten

Neben der manuellen Pflege können auch Strukturen aus anderen Bereichen eingefügt werden, z. B. ganze Äste aus dem «SAP-Menü» oder aus einer anderen Rolle.

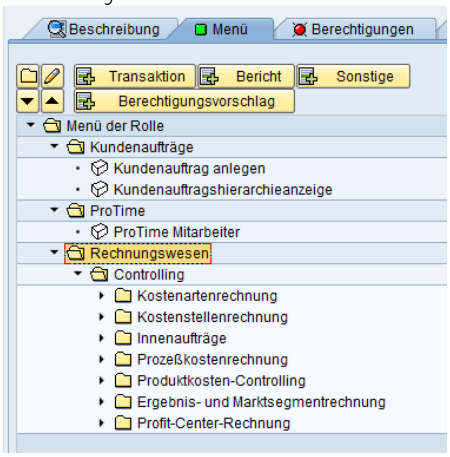


Wählen Sie die Drucktaste «SAP-Menü» und markieren im lokalen «SAP-Menü» den gesamten Bereich Controlling.



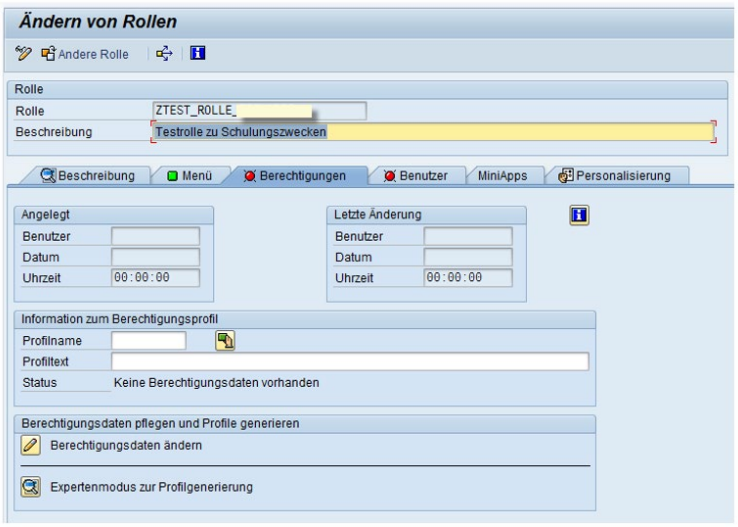
Bestätigen Sie Ihre Auswahl mit der Drucktaste «übernehmen» und der gesamte Teilbereich Controlling wird in die Rolle übernommen. Innerhalb der übernommenen Struktur können Sie in der Rolle nicht benötigte

Bereiche jederzeit eliminieren .



3.2.2. Berechtigungen pflegen

Wählen Sie das Register «Berechtigungen» und die Drucktaste « Berechtigungsdaten ändern».



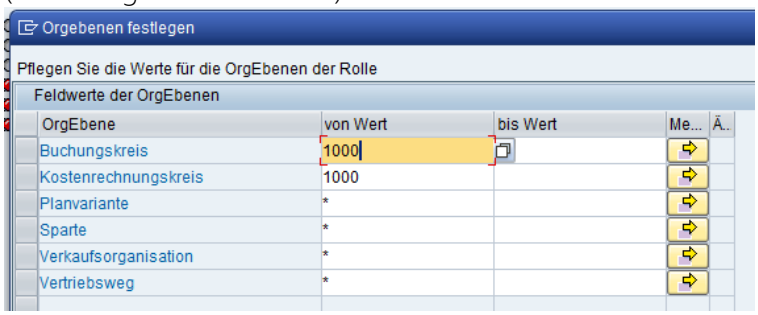
► Der **«Profilgenerator»** wird gestartet

Hinweis

Innerhalb des Profilgenerators müssen Sie die Berechtigungsobjekte ausprägen, die einer Transaktion zugeordnet sind, respektive gegebenenfalls zusätzliche Berechtigungsobjekte manuell in Ihre neue Rolle aufnehmen. Darüber hinaus müssen Sie je nach hinterlegten Transaktionen auch noch die Organisationseinheiten pflegen, auf die der Benutzer mit dieser Rolle Zugriff erhalten soll.

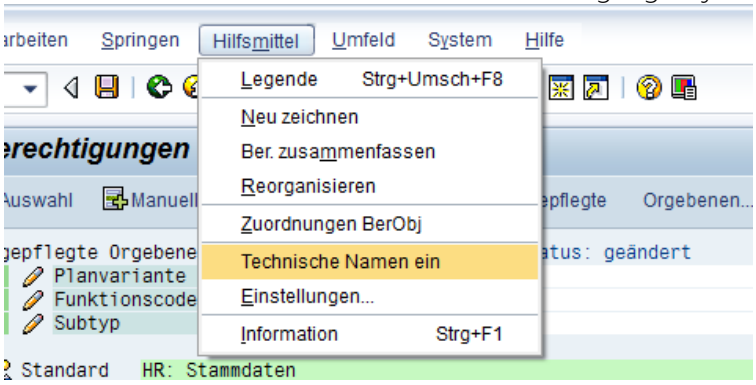
Sobald hinterlegte Transaktionen eine Prüfung auf Organisationseinheiten erfordern, werden Sie unmittelbar aufgefordert, diese zu pflegen.

Hinterlegen Sie einzelne Werte, Ranges, eine Mehrfachselektion oder die Gesamtberechtigung (in der Regel ein Sternchen) Gesamtberechtigung.

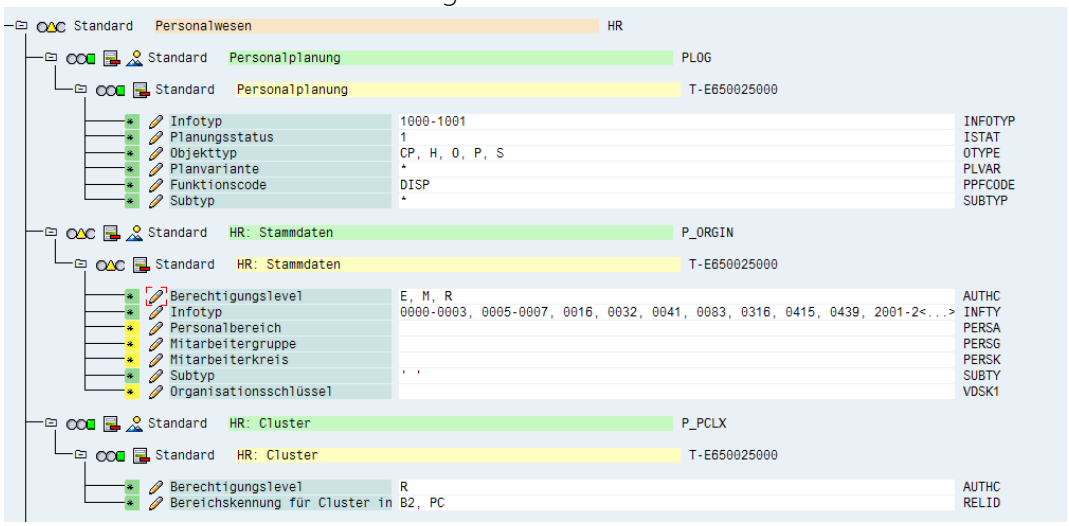


Erscheint bei der Berechtigungsübersicht eine gelbe oder rote «Ampel», so muss dieser Eintrag (Knoten) manuell nachgepflegt werden. Klappen Sie dazu den Baum auf .

Einblenden der technischen Namen der Berechtigungsobjekte: ► Menü Hilfsmittel / Technische Namen ein

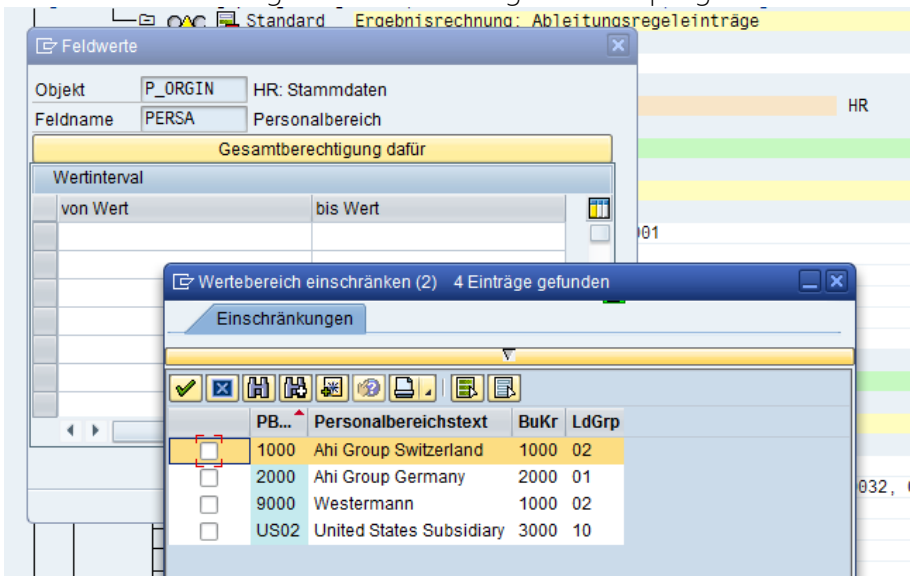


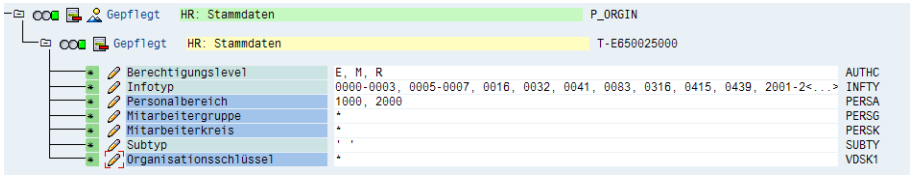
Im Berechtigungsobjekt **P_ORGIN** definieren Sie, auf welche Mitarbeitergruppen, Mitarbeiterkreise und Personalbereiche der Mitarbeiter zugreifen darf.



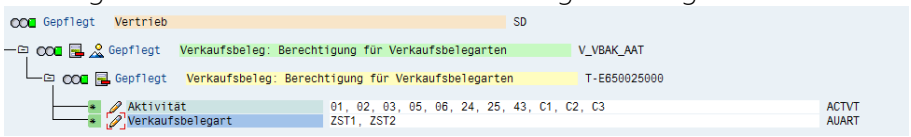
Durch Klick auf das «gelbe Sternchen» erteilen Sie eine «Gesamtberechtigung». Ein Klick auf den Bleistift startet dagegen die Pflegemaske für individuelle Einträge.

Darin können Sie die gewünschten Einträge manuell pflegen.



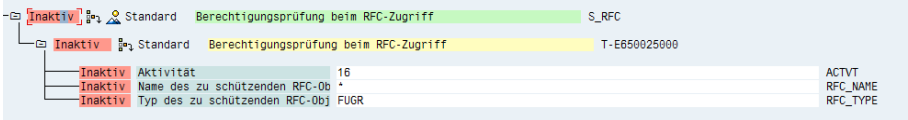


Der Zugriff sollte auf bestimmte Verkaufsbelegarten eingeschränkt werden ► kein «*».

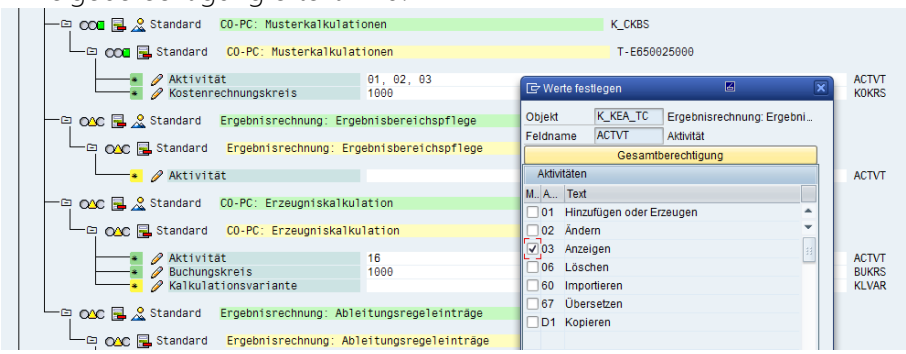


Wenn Sie ein Berechtigungsobjekt nicht kennen, können Sie dieses grundsätzlich erst einmal deaktivieren und später wieder aktivieren, falls es sich herausstellen sollte, dass es benötigt wird.

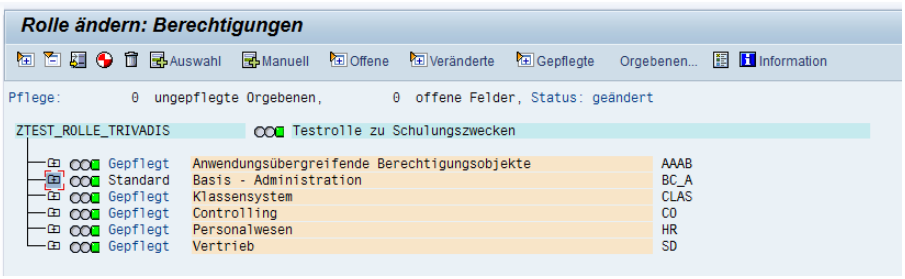
► Wählen Sie dazu die Drucktaste .



Innerhalb eines Berechtigungsobjekts können Sie vielfach auch die Aktivität dahingehend pflegen, dass nur Anzeigeberechtigung erteilt wird.



Pflegen Sie alle notwendigen Einträge gemäss Ihren Anforderungen.



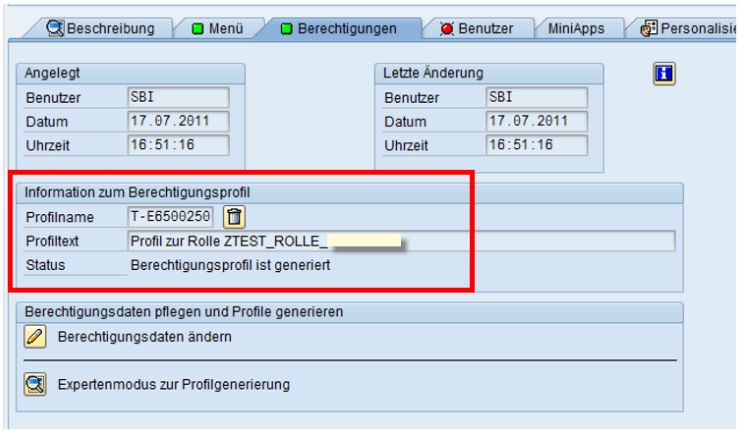
Wenn **alle** Einträge eine **«grüne Ampel»** haben, können Sie die Rolle sichern.

3.2.3. Berechtigungsprofil generieren

Eine Rolle ist nur dann konsistent, wenn aufgrund der definierten Berechtigungen auch ein entsprechendes Berechtigungsprofil generiert wurde. Eine Rolle kann jederzeit gesichert werden. Die Berechtigungen ziehen jedoch nur, wenn vorgängig ein aktuelles Berechtigungsprofil für die Rolle generiert wurde.

Wählen zur Generierung manuell die Drucktaste oder starten Sie diese, wenn Sie beim Sichern der Rolle dazu aufgefordert werden.

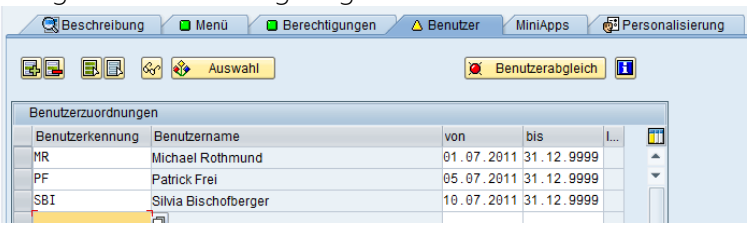
Wenn Sie die Rolle prüfen, ist das Register «Berechtigungen» mit einem grünen Symbol versehen und im Feld Profilname steht der generierte Profilnamen drin.



3.2.4. Benutzer zuordnen

Ist die Rolle konsistent, generiert wurde, können ihr Benutzer zugeordnet werden.

Im Register «Benutzer» können die gewünschten Benutzer für diese Rolle mit einem gewünschten Gültigkeitszeitraum eingetragen werden.



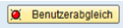
► anschliessend **unbedingt** «Benutzerabgleich» durchführen

Hinweis

Die Zuordnung von Rollen zu Benutzern kann auch über die Transaktion SU01 Benutzerpflege erfolgen.

3.2.5. Benutzerabgleich durchführen

Bei jeder Änderung einer Rolle sollte nicht nur das Berechtigungsprofil neu generiert werden, sondern auch ein Benutzerabgleich durchgeführt werden. Nur so kann sichergestellt werden, dass die Rolle vollständig greift und die aktuellen Berechtigungen darin für die Benutzer ziehen.

Wählen Sie im Register «Benutzer» die Drucktaste 

. Erst dann wird das Symbol auf dem Register «Benutzer» grün.

Hinweis

Der Benutzerabgleich wird normalerweise auch über einen Nachtjob periodisch für alle Rollen durchgeführt. Dazu muss der Report PFCG_TIME_DEPENDENCY (Massenabgleich) in einem periodischen Job eingeplant und ausgeführt werden.

3.3. Rolle ändern ► Schritte im Detail

Bei Bedarf können Rollen ergänzt oder z.B. auch eine Berechtigung gelöscht werden.

Hinweis

Änderungen in bestehenden Rollen wirken sich auf alle Benutzer aus, die diese Rolle zugeordnet haben. Prüfen Sie genau, in welcher Rolle Sie Änderungen vornehmen.

Beachten Sie, dass Berechtigungen innerhalb SAP immer additiv wirken, d. h. wenn Sie innerhalb einer Rolle die Berechtigung zum Anlegen von Kundenaufträgen im Buchungskreis 1000 haben und durch eine andere Rolle die Berechtigung zum Anzeigen von Fakturen des Buchungskreises 2000 haben, kann es durch eine entsprechende Konstellation beider Rollen durchaus vorkommen, dass Sie dadurch die Berechtigung im Buchungskreis 1000 und 2000 zum Anlegen von Kundenaufträgen und Anzeigen von Fakturen haben.

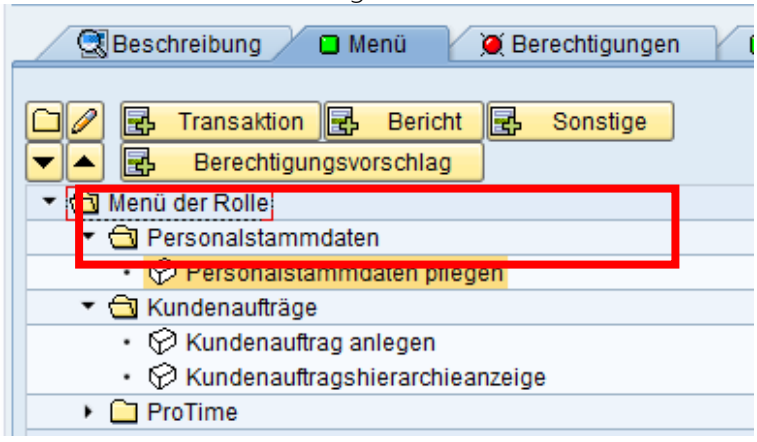
Nachfolgend der Grobablauf beim Ändern einer bestehenden Rolle.

- neue Transaktion hinzufügen oder
  zusätzliche Berechtigungsobjekte und deren Ausprägung manuell hinzufügen
- Rolle manuell nachbearbeiten
- Organisatorische Zuordnungen immer über das OrgFenster pflegen,
  damit diese in alle Berechtigungsobjekte vererbt werden
- Berechtigungsprofil neu generieren
- Benutzerabgleich durchführen

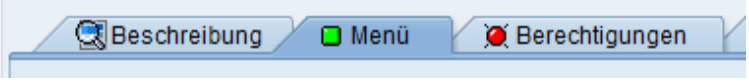
3.3.1. Transaktion hinzufügen

Transaktion PFCG Rollenpflege aufrufen und zu ändernde Rolle eingeben.

Die neue Transaktion an der gewünschten Stelle in der Menüstruktur einfügen.



Das Register «Berechtigungen» wechselt auf **«rot»**.

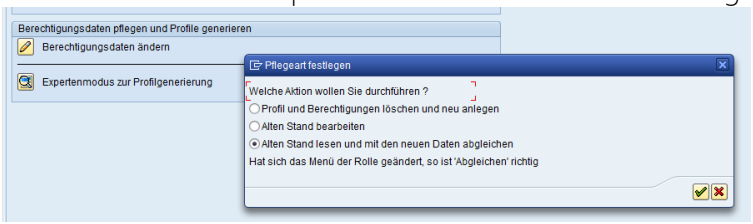


3.3.2. Berechtigungsdaten ändern

Es erfolgt automatisch ein Abgleich der alten Profilwerte mit den aktuellen Vorschlagswerten für die bereits vorhandenen und neu hinzugefügten Transaktionen. Dabei werden alle Berechtigungsobjekte entzogen, die nicht dem aktuell über das Menü festgelegten transaktionalen Umfang der Rolle entsprechen, sofern die zugehörigen Berechtigungsobjekte im Profil nicht den Status «manuell» oder «geändert» aufweisen.

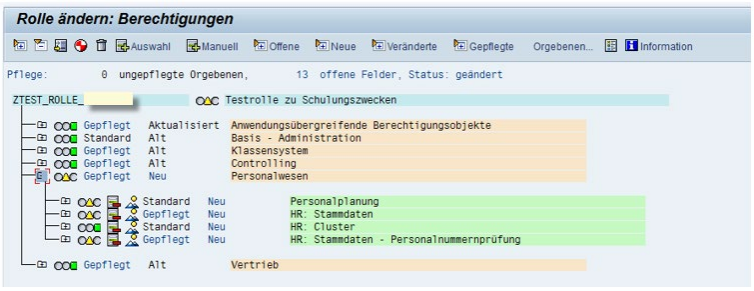
Hinweis

Über die Drucktaste «Expertenmodus» kann direkt eine Pflegeart festgelegt werden.

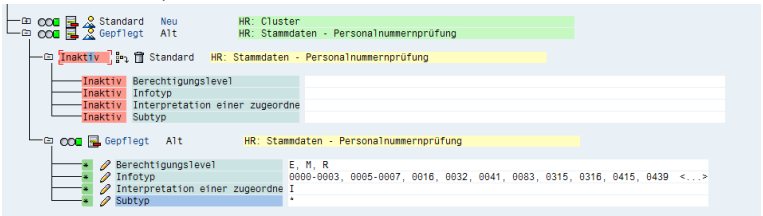


Wählen Sie die Option «alten Stand lesen und mit neuen Daten abgleichen».

Da die Rolle bereits generiert war, müssen Sie nur noch für die neu hinzugefügte Transaktion die entsprechenden Berechtigungsobjekte oder organisatorischen Einheiten pflegen (► gelbe Ampeln).



Beachten Sie, dass es durchaus vorkommen kann, dass mehrere Transaktionen innerhalb einer Rolle die gleichen Berechtigungsobjekte nutzen. Damit diese nicht mehrfach gepflegt werden (ggf. sogar unterschiedlich), können Sie einen doppelten Eintrag deaktivieren (und anschliessend – sofern gewünscht – auch löschen).



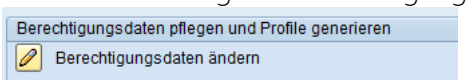
3.3.3. Berechtigungsobjekte manuell pflegen

Sollte in einer Rolle ein Berechtigungsobjekt fehlen oder die Ausprägung überprüft und angepasst werden, muss dies im **«Profilgenerator»** erfolgen.

Analysieren Sie über die Berechtigungsreports, in welcher Rolle die gewünschte Transaktion oder das Berechtigungsobjekt enthalten ist. Respektive überlegen Sie, in welcher Rolle Sie das fehlende Berechtigungsobjekt nachtragen möchten. Es ist möglich, dass ein Benutzer über mehrere Rollen ein Berechtigungsobjekt mehrfach zugeordnet hat, da ein Berechtigungsobjekt mehreren Transaktionen standardmässig als Vorschlagswert zugeordnet ist.

Transaktion PFCG Rollenpflege aufrufen und zu ändernde Rolle eingeben.

Wählen Sie im Register «Berechtigungen» die Drucktaste «Berechtigungsdaten ändern».

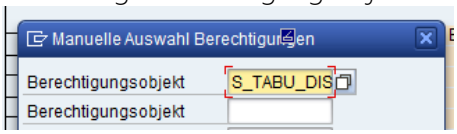


► Der **«Profilgenerator»** wird gestartet

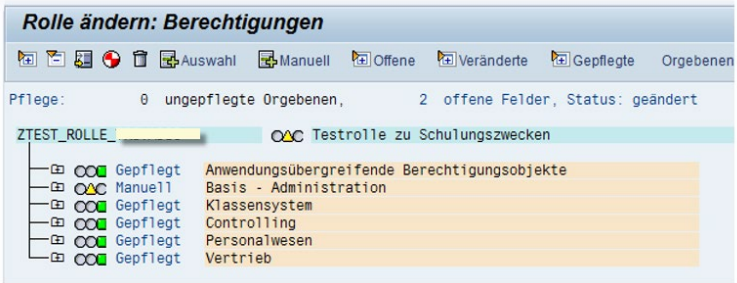
Wählen Sie die Drucktaste «Manuell» 

, um zusätzliche Berechtigungsobjekte hinzuzufügen.

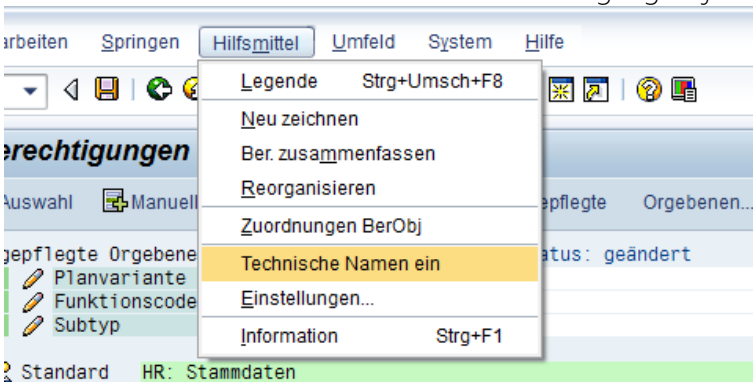
► benötigte Berechtigungsobjekte eingeben



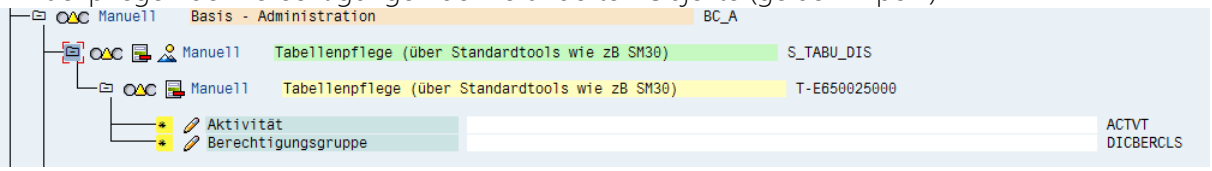
Die Rolle enthält anschliessend wieder gelbe Einträge, die nachbearbeitet werden müssen.

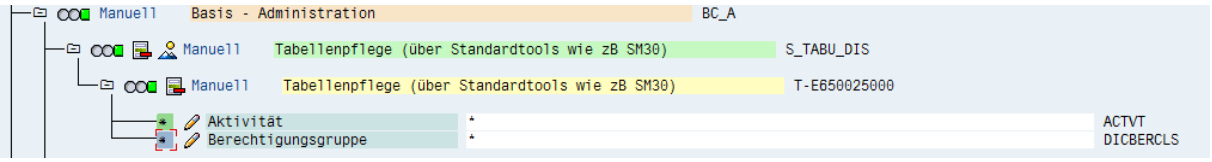


Einblenden der technischen Namen der Berechtigungsobjekte: ► Menü Hilfsmittel / Technische Namen ein



► nachpflegen der Berechtigungen der veränderten Objekte (gelbe Ampeln)





3.3.4. Berechtigungsprofil generieren

Nach Änderung der Berechtigungen muss das Berechtigungsprofil neu generiert werden.

3.3.5. Benutzerabgleich durchführen

Nach Änderung des Berechtigungprofils muss erneut ein Benutzerabgleich durchgeführt werden.

4. Fiori Launchpad

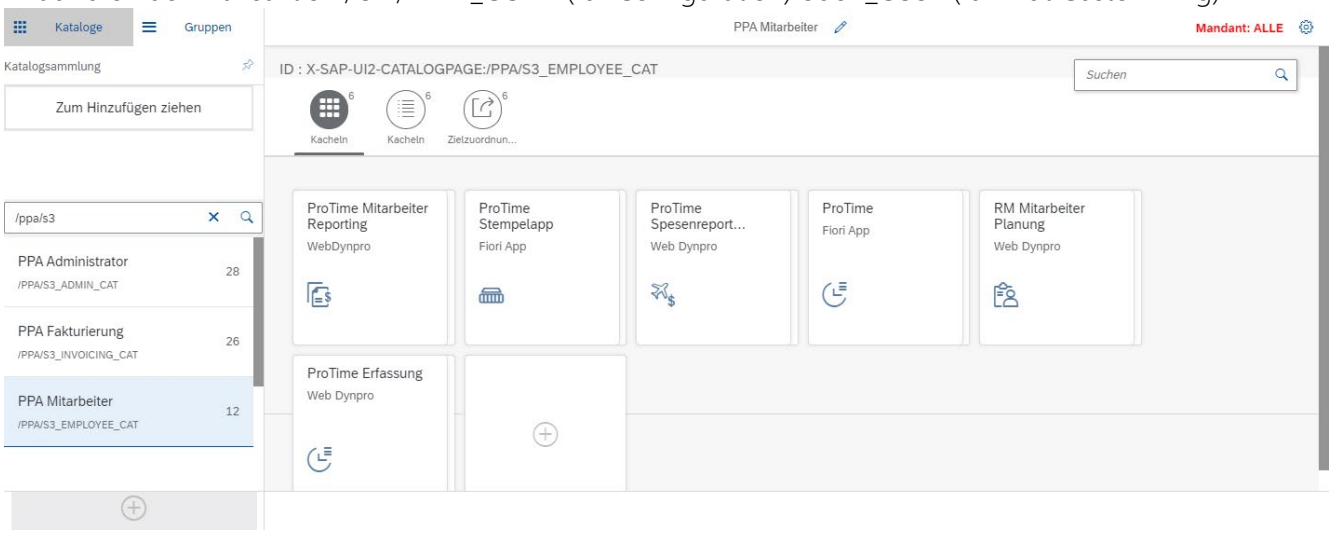
4.1. Fiori Kataloge und Gruppen pflegen

Fiori Kataloge können entweder im Fiori Designer (Launchpad) oder aber im Fiori Analyse-Werkzeug (siehe sep. Kapitel) bearbeitet werden. Fiori Gruppen hingegen sind nur über den Fiori Designer zu bearbeiten.

Der Fiori Designer bietet z.B. folgende Funktionen.

- Übersicht der Kataloge sowie der darin erstellten Zielzuordnungen und Kacheln
- Übersicht der Gruppen sowie der darin zugeteilten Kacheln (aus Katalogen)
- Pflege der Zielzuordnungen und Kacheln mit visueller Überprüfung (Icons, Titel/Subtitel, Darstellung)

► aufrufen der Transaktion /UI2/FLPD_CONF (für Configuration) oder _CUST (für Mdt Customizing)

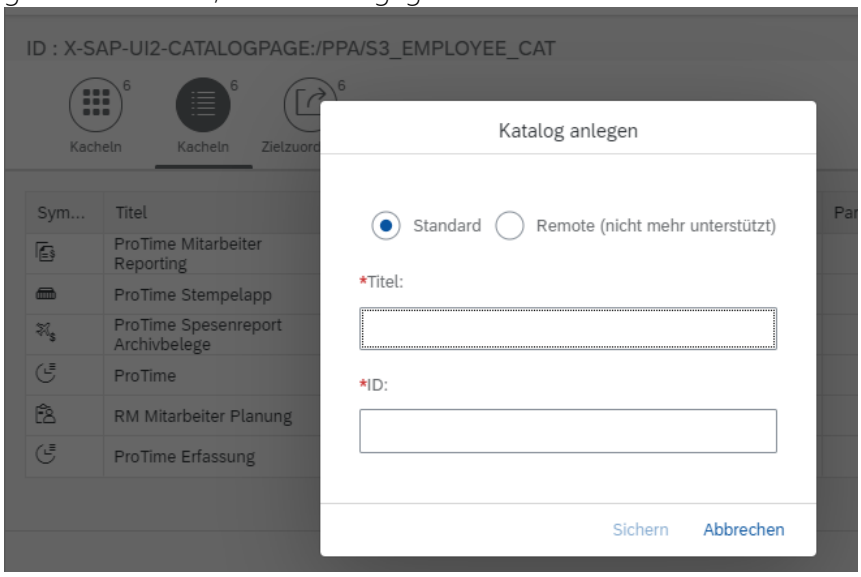


Link oben wird zwischen der Verwaltung von Katalogen und Gruppen gewechselt. Die ausgewählte Funktion ist grau hinterlegt.

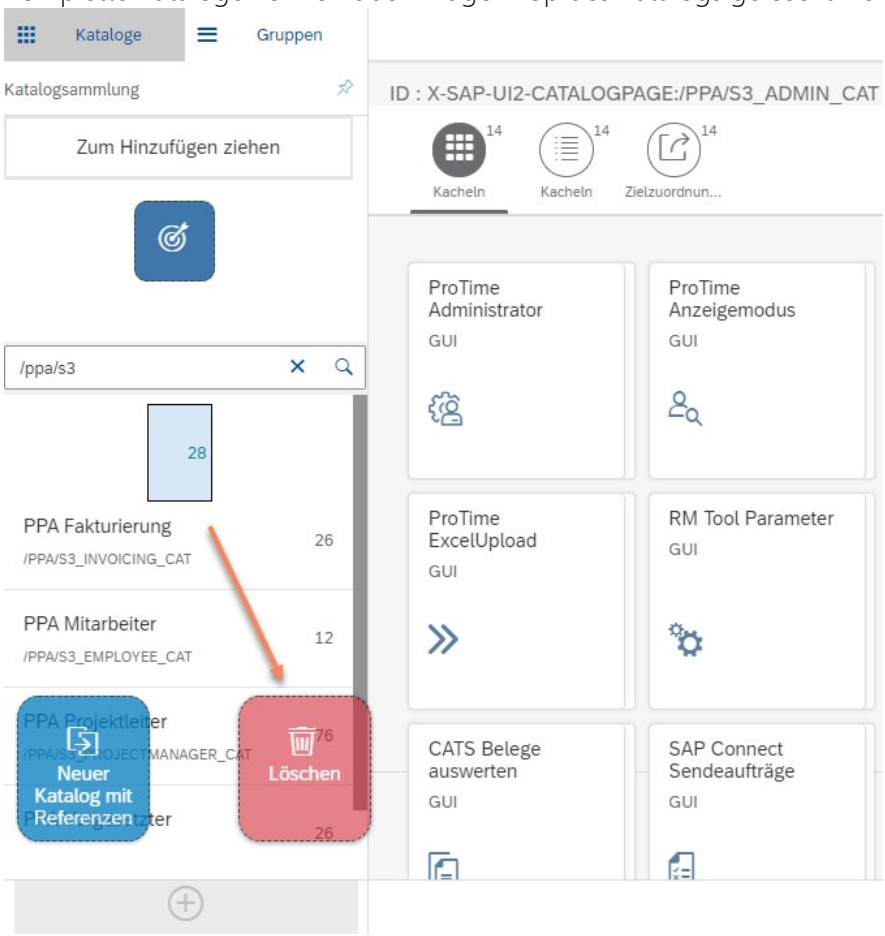
4.1.1. Kataloge pflegen

Am linken Bildrand werden die Kataloge aufgelistet, über die Suchfunktion können Einschränkungen durchgeführt werden. Durch die Selektion eines Katalogs in der Liste wird im rechten Fenster der Inhalt verfügbar.

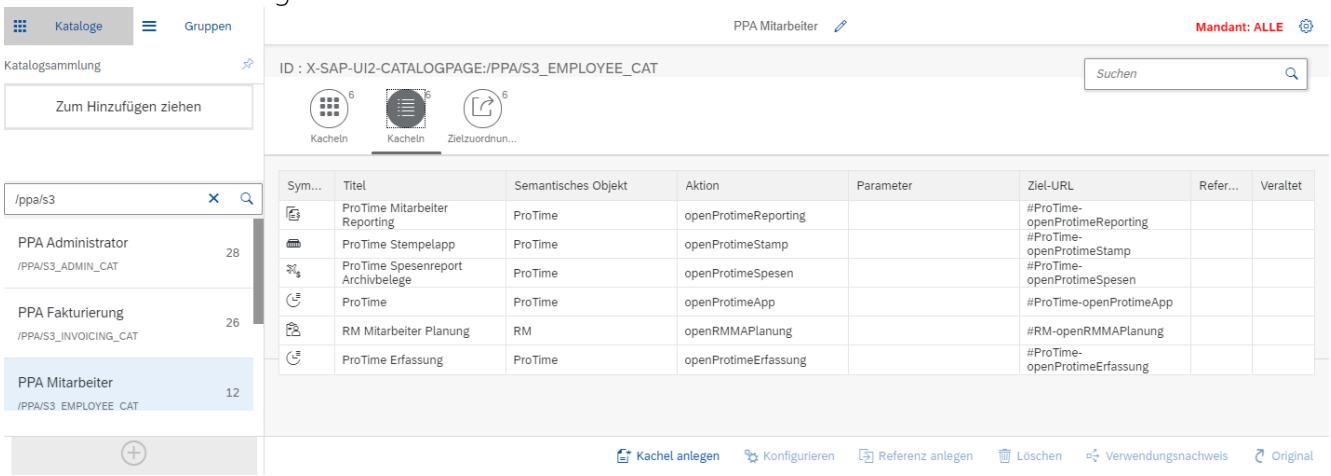
Neue Kataloge werden über das Plus-Symbol (links unten) erstellt. Die ID kann nachträglich nicht mehr geändert werden, der Titel hingegen ist änderbar



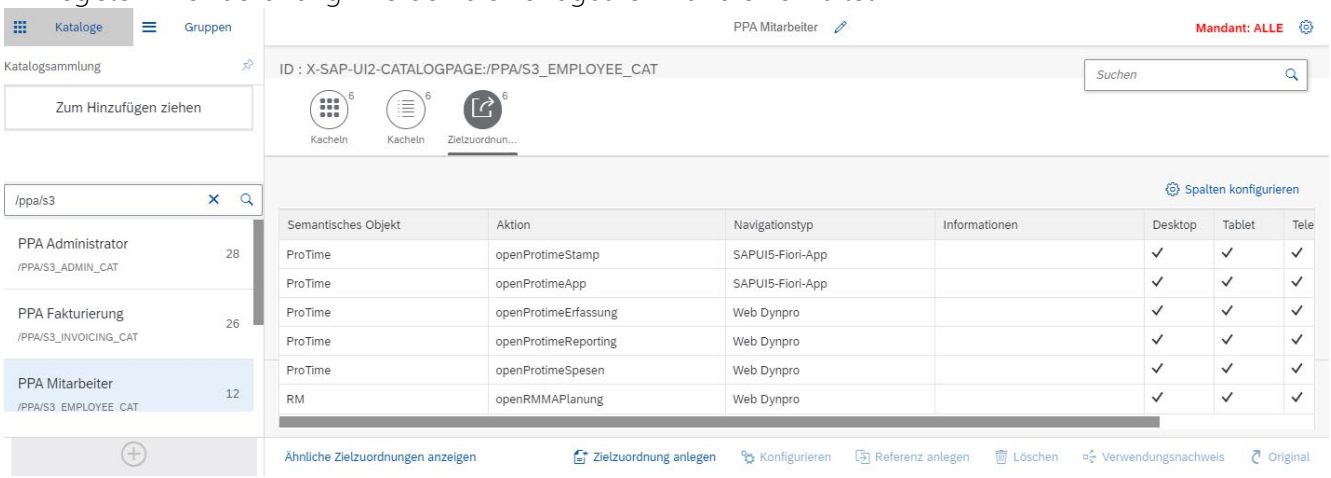
Komplette Kataloge können über Drag&Drop des Katalogs gelöscht werden



In den beiden «Registern» Kacheln werden die im selektierten Katalog verfügbaren Kacheln in grafischer oder in Listenform aufgeführt.

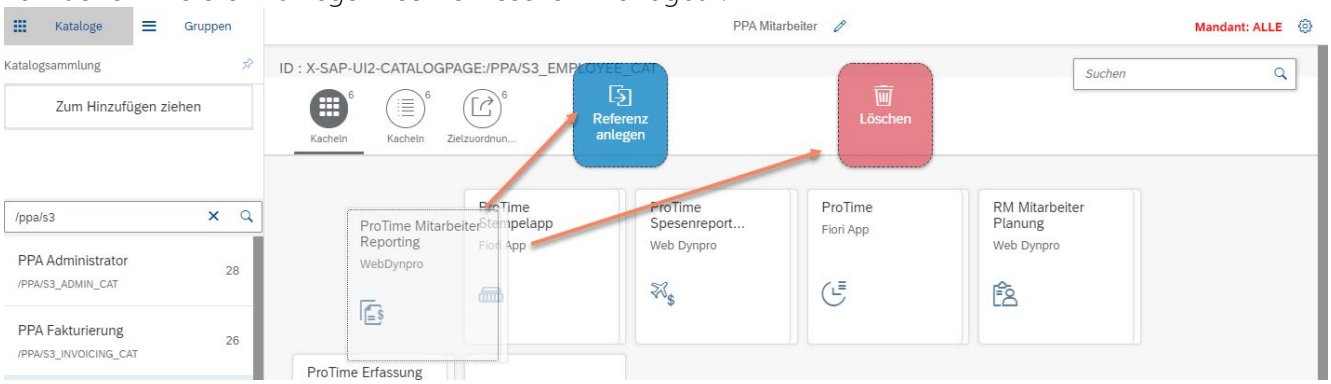


Im Register «Zielzuordnung» werden die verfügbaren Aufrufe verwaltet



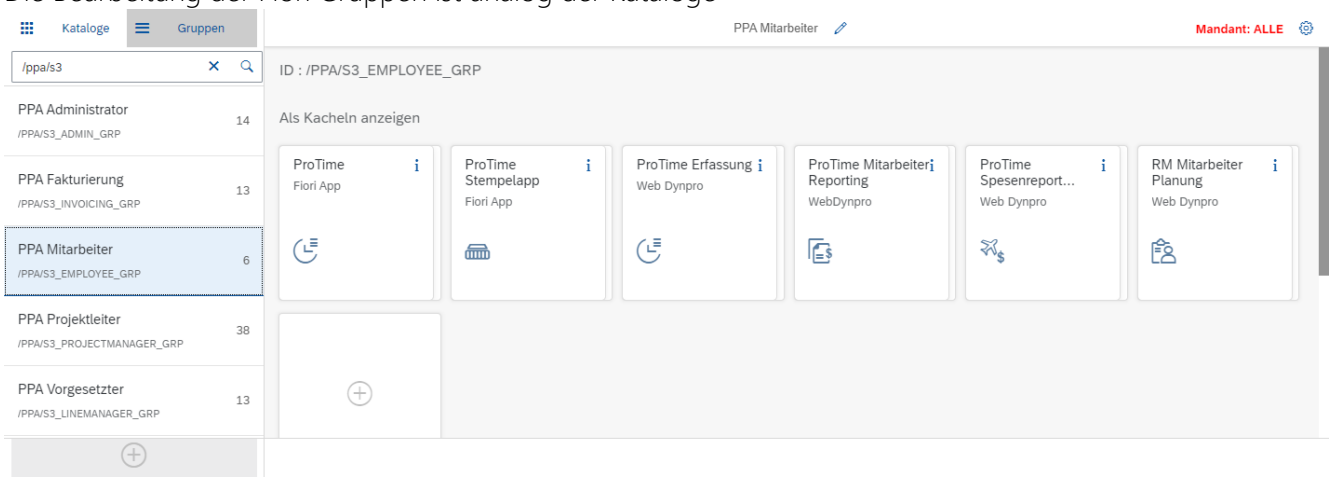
Funktionen im Fiori Designer in den Listendarstellungen sind um unteren Bildrand als Buttons aufgeführt. Dazu gehören unter anderem Funktionen wie «Kachel anlegen», «Referenz anlegen», «löschen», «Zielzuordnung anlegen», etc.

In der grafischen Darstellung der Kacheln steht kein Funktionsband dargestellt. Mittels Drag&Drop sind die Funktionen «Referenz anlegen» sowie «löschen» verfügbar.

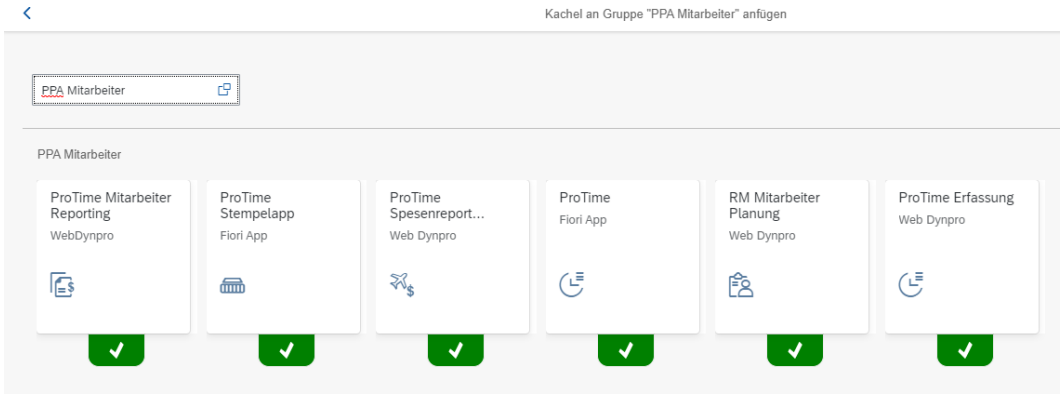


4.1.2. Gruppen pflegen

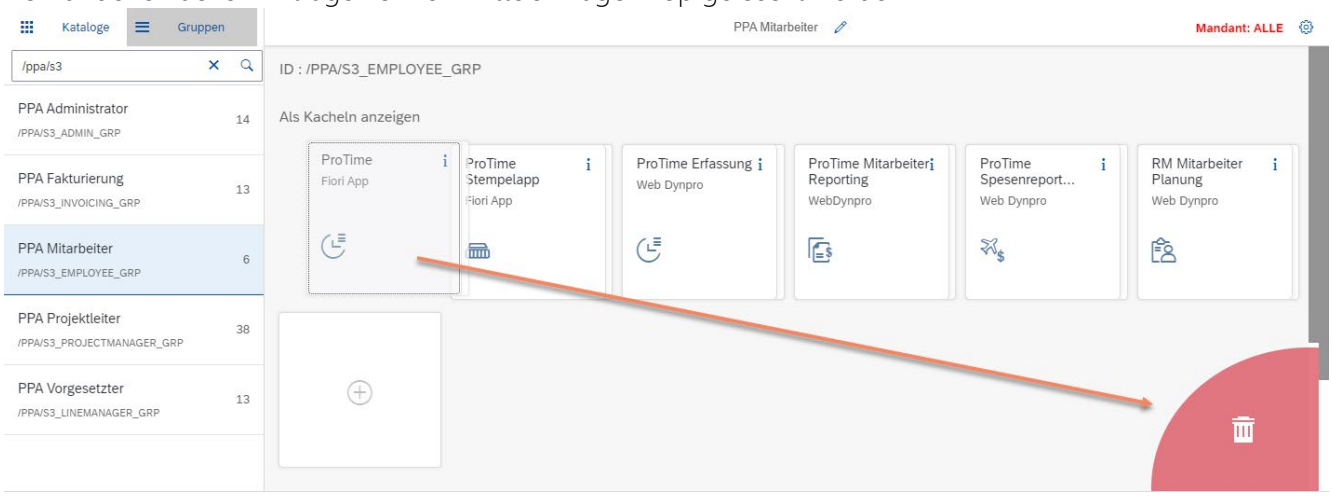
Die Bearbeitung der Fiori Gruppen ist analog der Kataloge



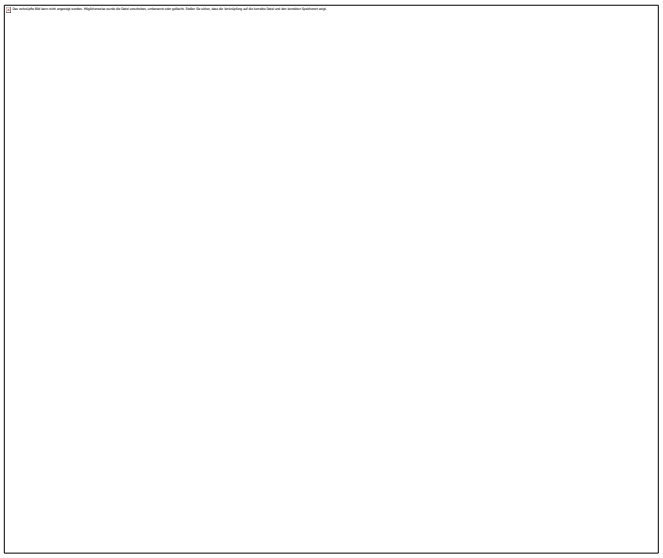
Neue Kacheln in Gruppen werden über das Plus-Symbol hinzugefügt. Dazu muss zuerst der Ursprungskatalog gesucht werden, im zweiten Schritt können über die gewünschten Kacheln markiert und übernommen werden



Vorhandene Kachel-Einträge können mittels Drag&Drop gelöscht werden



Fiori Gruppen haben eine Einstellung, welche sich bei den Benutzern in die Bearbeitung der Startseite auswirkt:



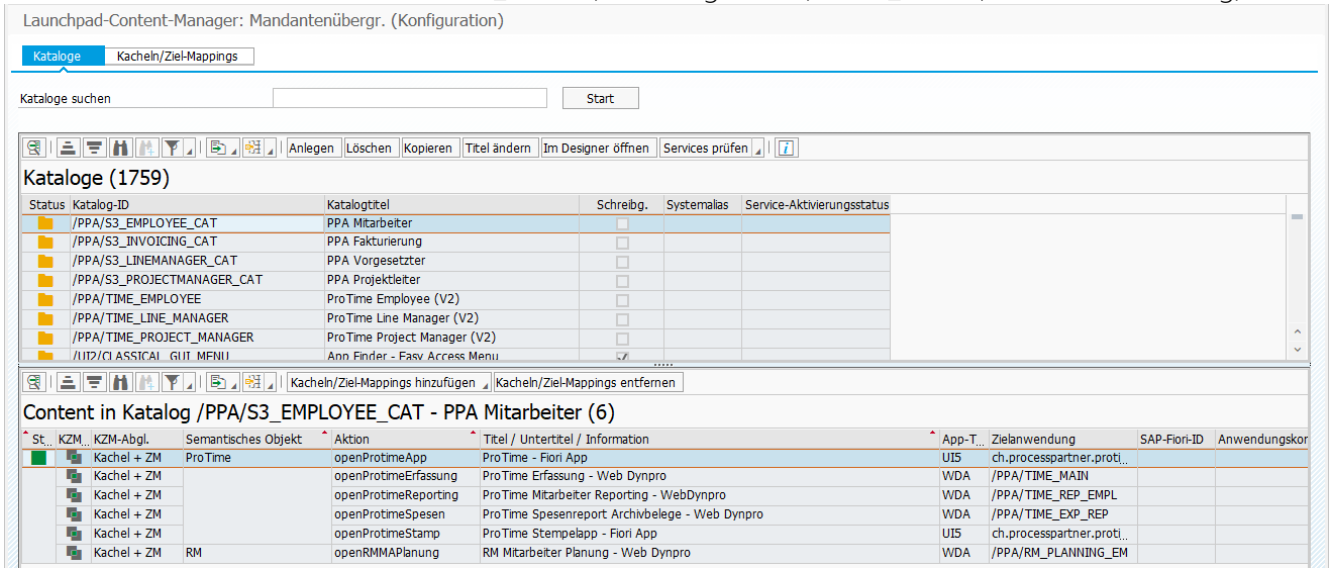
Wird diese Möglichkeit nicht aktiviert, so wird diese Gruppe im Fiori Launchpad an erster Stelle vor der Gruppe «Meine Startseite» aufgeführt und ist weder in der Reihenfolge noch inhaltlich änderbar.

4.2. Fiori Kataloge analysieren und verwalten

Diese Transaktion bietet z.B. folgende Funktionen.

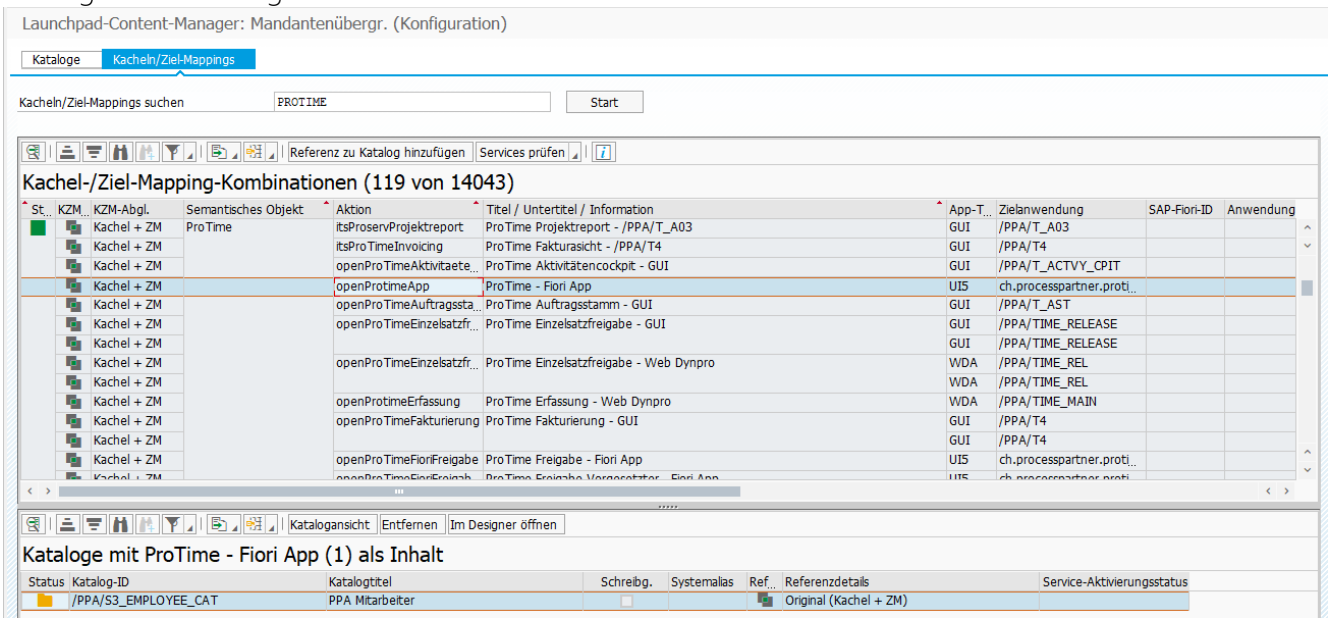
- Übersicht der Katalog sowie der darin erstellten Zielzuordnungen und Kacheln
- Erkennung von Fehlern
- Erstellte Zielzuordnungen und Kacheln in andere Kataloge hinzufügen
- Bei Bedarf können neue Katalog erstellt, Kataloge umbenannt oder Kataloge gelöscht werden
- Kacheln können zwischen Katalogen als Referenzen kopiert und eingefügt werden

► aufrufen der Transaktion /UI2/FLPCM_CONF (für Configuration) oder _CUST (für Mdt Customizing)



Im Register «Kataloge» werden die Kataloge aufgelistet und je selektiertem Katalog im unteren Fenster die darin enthaltenen Kacheln und Zielzuordnungen (ZM) dargestellt.

Im Register «Kacheln/Ziel-Mappings» ist die umgekehrte Sicht. Je Kachel wird aufgelistet, in welchen Katalogen diese verfügbar ist.



Hinweis

Kataloge und Kacheln werden üblicherweise in der Configuration (Mdt-übergreifend) erstellt und verwaltet und bei Bedarf im Customizing (Mdt-spezifisch) angepasst oder ausgeblendet.

4.3. SAP Standard Apps auffinden und in eigene Kacheln/Gruppen übernehmen

Ausgelieferte Standard-Apps der SAP können nach gleichen Mechanismen in eigenen Katalog und/oder Gruppen übernommen werden. Wichtig hierzu ist die Kenntnis der Fiori App-ID, diese kann im Benutzermenü des Launchpads über die Funktion «Info / Über» ausgelesen werden

Anhand dieser App-ID sind erweiterte Informationen bei der SAP in der Fiori App Library zu finden (https://fioriappslibrary.hana.ondemand.com/sap/fix/externalViewer/). Diese listet unter anderem folgende Informationen:

- Angaben zum ausgelieferten Katalog / Gruppe
- Angaben zur ausgelieferten SAP BusinessRole
- Angaben zu speziellen Berechtigungseinstellungen
- …

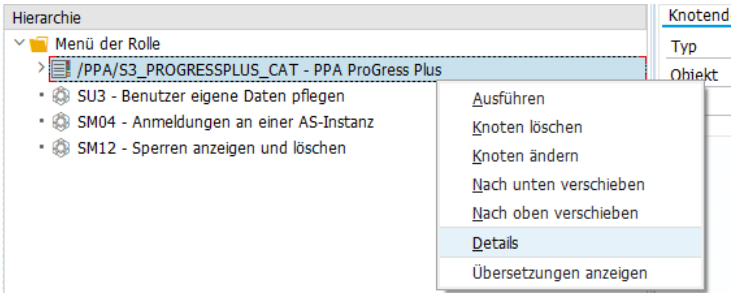
Eine Standard-App kann nun mit den oben aufgeführten Werkzeugen in den eigenen Katalog/Gruppen ergänzt werden.

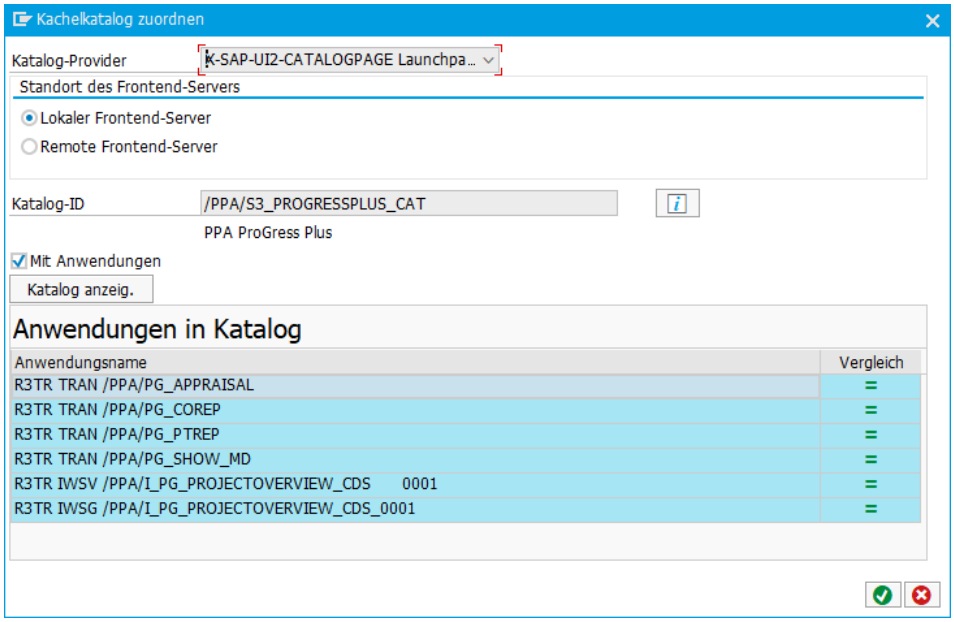
4.4. Abgleich Benutzerrollen nach Anpassungen von Fiori Katalogen

Wenn in SAP Fiori Kachelkataloge angepasst werden, so müssen auch die zugehörigen Rollen aktualisiert werden. Dies kann entweder ausgehend von der Rolle oder als Massenabgleich stattfinden.

4.4.1. Prüfung Rolle auf Änderungen von Fiori Katalogen

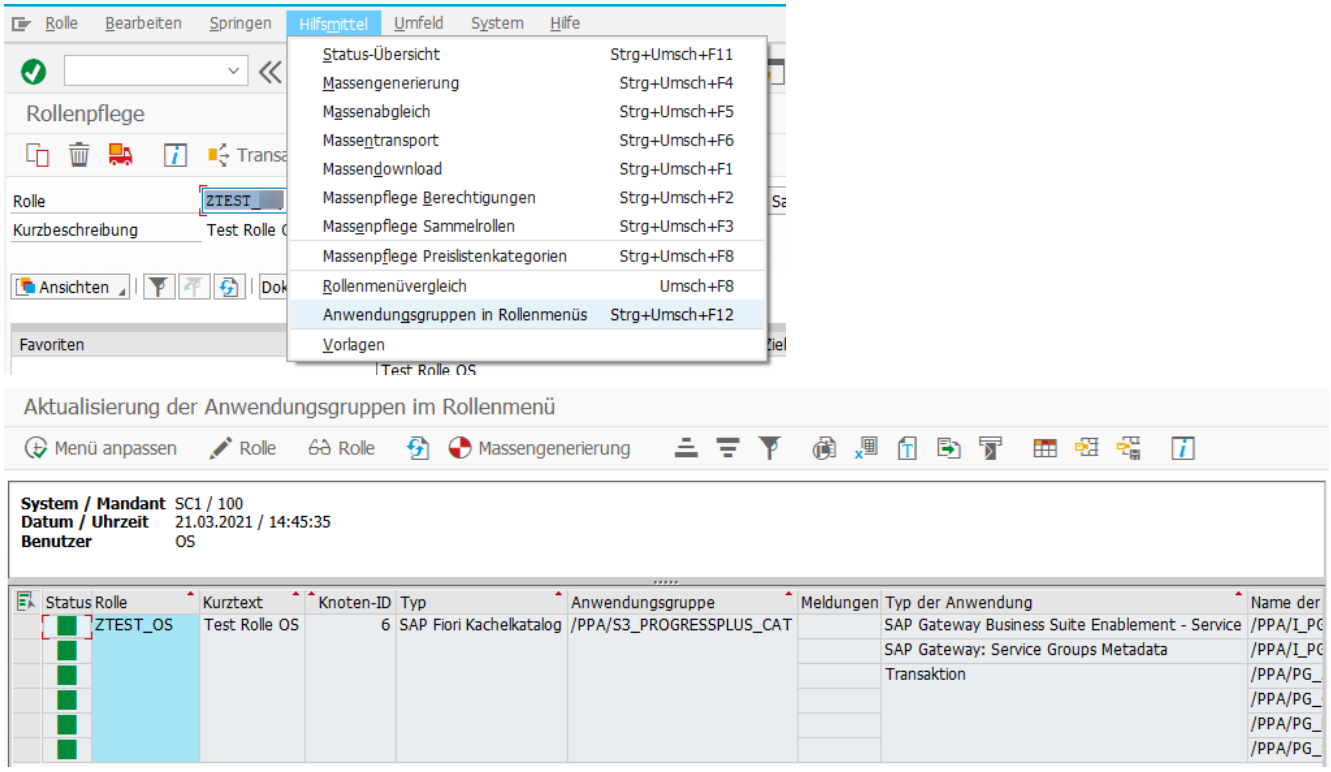
Ausgehend von der Rolle kann über das Kontextmenü des Katalogs über Details ein Statusabgleich durchgeführt und im Anschluss korrigiert werden:





4.4.2. Massenabgleich Änderungen von Fiori Katalogen

Die Prüfung kann entweder über Aufruf des Programms «PRGN_COMPARE_ROLE_MENU» (mittels SE38) oder aus der PFCG heraus über Hilfsmittel / Anwendungsgruppen in Rollenmenüs gestartet und durchgeführt werden:



5. Analyse Berechtigungsfehler

5.1. Anfrage «Fehlende Berechtigung»

Erhält man eine Mitteilung, es fehle eine Berechtigung oder wird eine zusätzliche Berechtigung beantragt, so kann dies verschiedene Ursachen haben.

- Der Benutzer benötigt Zugriff auf eine Transaktion, die bisher nicht in seinen Rollen enthalten war.
- Der Benutzer benötigt innerhalb einer zugewiesenen Transaktion erweiterte Berechtigungen, weil z.B. ein Berechtigungsobjekt nicht ausreichend ausgeprägt ist.

Vorgehen

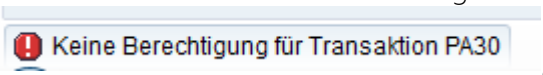
- einfordern beim Benutzer, welche Berechtigung fehlt ► siehe «Berechtigungsdaten anzeigen»
- prüfen, ob der Benutzer bereits für die Transaktion berechtigt ist ► siehe «Ausführbare Transaktionen»
- prüfen, in welchen Rollen die Transaktion enthalten ist ► siehe «Rollen nach Transaktionszuordnung»
- liefert die Transaktion «SU53 Berechtigungsdaten anzeigen» nicht die relevanten Infos, kann ein Berechtigungstrace durchgeführt werden ► siehe «Berechtigungstrace»

5.2. Transaktion SU53 Berechtigungsdaten anzeigen (Analyse-Werkzeug)

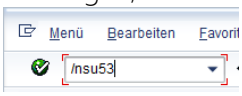
Diese Transaktion bietet z.B. folgende Funktionen.

- Detailprotokoll nach Fehlermeldung «Keine Berechtigung . . .»

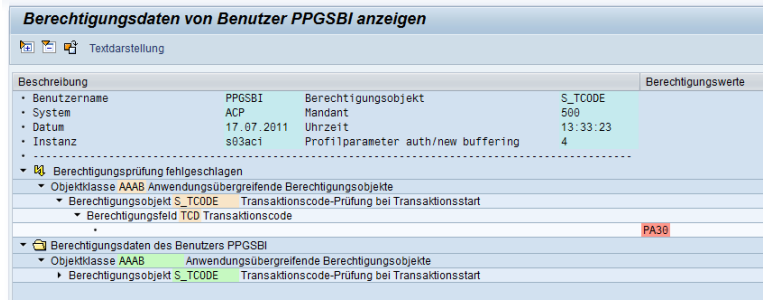
Erhält ein Benutzer eine Fehlermeldung



so sollte er unmittelbar nach der Fehlermeldung im Befehlsfeld **/nsu53** eingeben und mit «**Enter-Taste**» bestätigen, um sich die Berechtigungsdaten anzeigen zu lassen.



Beispiel A: Versuch, die Transaktion PA30 (Personalstammdaten pflegen) aufzurufen.

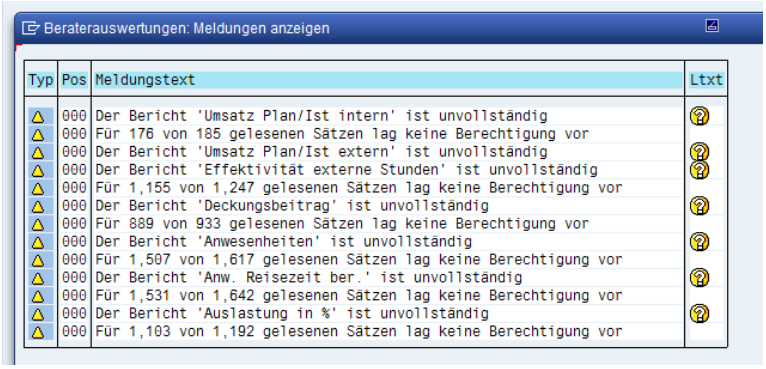


Analyse

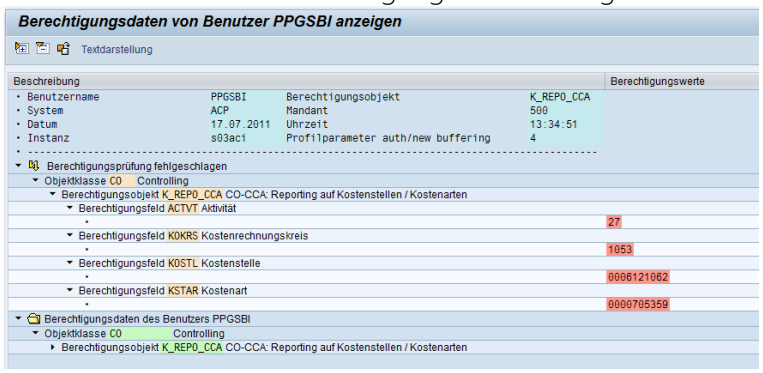
Dem Benutzer fehlt die Berechtigung für Transaktion PA30.

► Berechtigungsobjekt **S_TCODE**, Ausprägung Transaktionscode **PA30**

Beispiel B: Aufruf eines Reports ► Benutzer erhält folgende Fehlermeldung.



Die Transaktion «SU53 Berechtigungsdaten anzeigen» liefert folgendes Ergebnis.



Im Berechtigungsobjekt K_REPO_CCA müssen

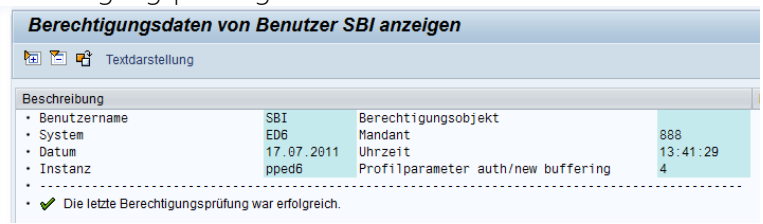
- die Aktivität 27 nachgetragen werden
- Zugriff für den Kostenrechnungskreis 1053
- Zugriff auf die Kostenstelle 6121062
- Zugriff auf die Kostenart 705359

erteilt werden.

Es ist im Folgenden daher eine Berechtigungsrolle zu definieren, innerhalb derer diese Informationen nachgetragen werden.

Hinweis

Es ist möglich, dass dem Benutzer weitere Berechtigungen fehlen. Nachdem eine Rolle mit diesen Berechtigungen dem Benutzer zugeordnet wurde, sollte der Benutzer entsprechend prüfen, ob die Funktion nun korrekt ausgeführt werden kann. Andernfalls muss der Analyseweg über Transaktion «SU53 Berechtigungsdaten anzeigen» mehrmals hintereinander durchgeführt werden, bis die Berechtigungsprüfung nicht mehr auf Fehler läuft.



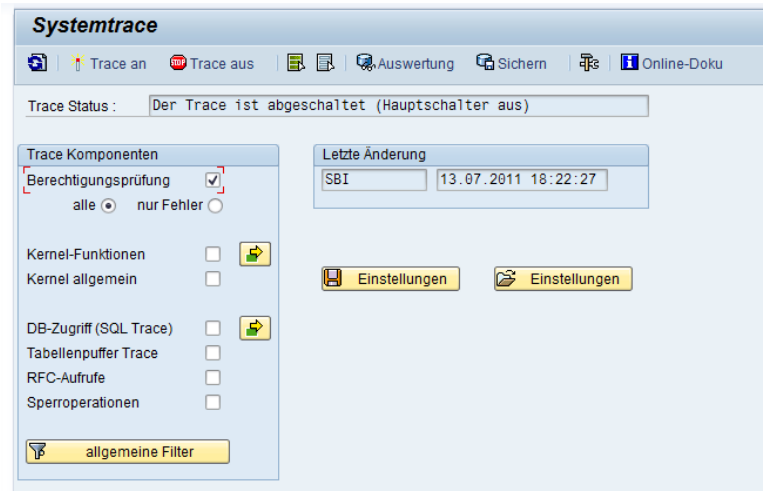
5.3. Transaktion ST01 SAP System Trace

Diese Transaktion bietet z.B. folgende Funktionen.

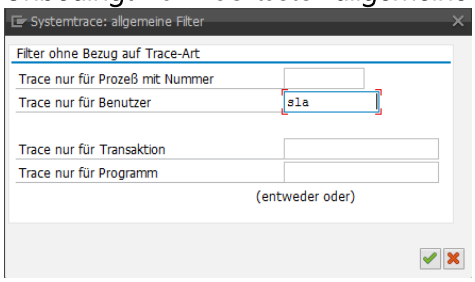
- Berechtigungstrace durchführen, wenn z.B. Transaktion SU53 zu wenig Infos lieferte

5.3.1. Konfigurieren Berechtigungstrace

- ausführen Transaktion «ST01 Systemtrace»
- markieren «Berechtigungsprüfung»
- wählen «alle Prüfungen» oder «nur Fehler (nicht erfolgreiche Prüfungen)»



Unbedingt via Drucktaste **«allgemeine Filter»** das Trace auf einen bestimmten Benutzer einschränken.



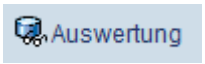
► Trace einschalten

► Der betroffene Benutzer sollte im «SAP-Menü» nun genau die Schritte durchführen, die zur negativen Berechtigungsprüfung führt (möglichst nicht zu viele Schritte durchführen, da alles aufgezeichnet wird, daher möglichst im Prozess erst kurz vor dem Berechtigungsfehler das Trace §einschalten).

► Trace ausschalten

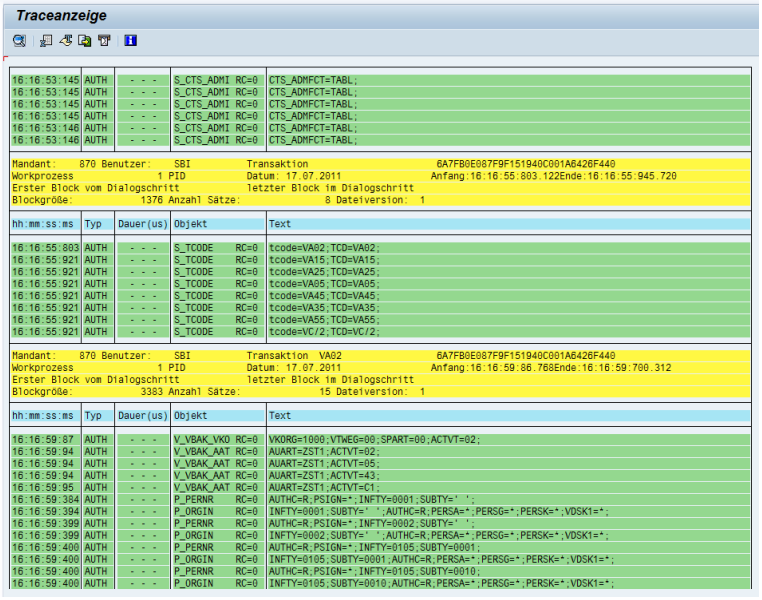
►W I C H T I G, nicht vergessen!!!! ☺

Trace-Protokoll anzeigen



Die Trace-Sätze auf Benutzer, Berechtigungsprüfungen und ggf. auf «nur Fehler» einschränken.

Das Protokoll liefert Hinweise darauf, welche Berechtigungsprüfungen durchgeführt wurden.



Das Ergebnis der Transaktion VA02 und dem Aufruf eines Kundenauftrags. Dabei werden z.B. Berechtigungsobjekte S_TCODE, P_PERNR, P_ORGIN etc. aufgerufen, Organisationseinheiten geprüft etc.

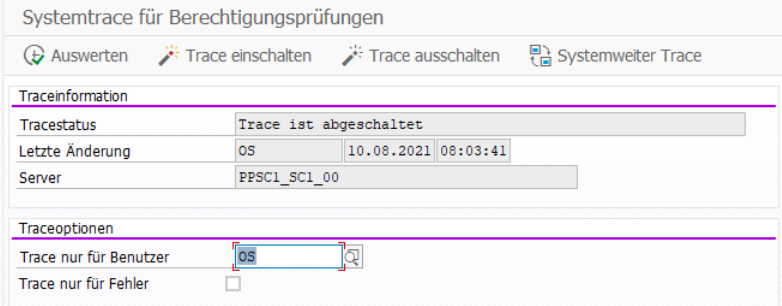
5.4. Transaktion STAUTHTRACE Berechtigungstrace

Diese Transaktion bietet Traceaufnahmen spezifisch zu Berechtigungen an. Dies ist als Spezialisierung der allgemeinen Systemtrace (ST01) zu betrachten. Dieses Tool drängt sich u.A. dafür auf, wenn für Services und Hintergrundjobs spezifische Berechtigungen massgeschneidert werden sollen. So können über das GUI die Aktionen ausgeführt und in eine spezifische Berechtigungsrolle übernommen werden.

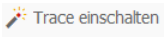
5.4.1. Konfigurieren Berechtigungstrace

- ausführen Transaktion «STAUTHTRACE Berechtigungstrace»

- In Trace-Optionen gewünschten Benutzer eintragen
- Optional Auswahl «Trace nur für Fehler»



► Trace einschalten

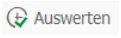


► Der betroffene Benutzer sollte im «SAP-Menü» nun genau die Schritte durchführen, die ausgewertet werden sollen.

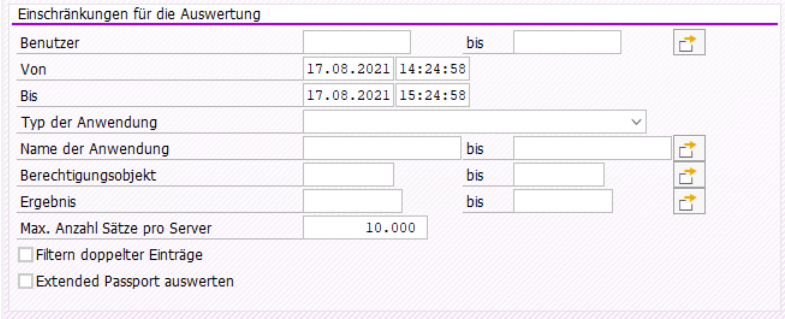
► Trace ausschalten

►W I C H T I G, nicht vergessen!!!! ☺

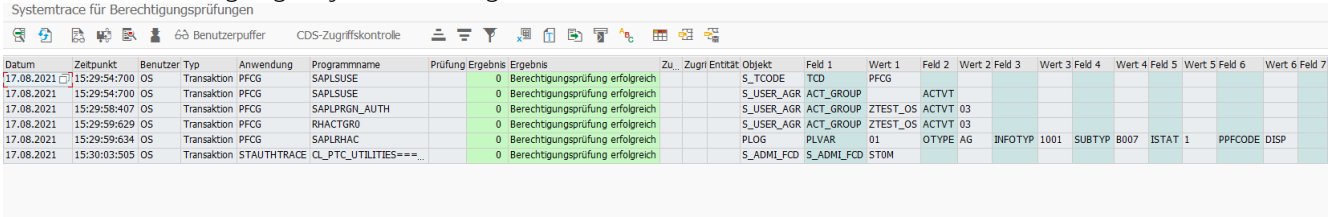
Trace-Protokoll anzeigen



Die Trace-Sätze können bei Bedarf weiter eingeschränkt werden:

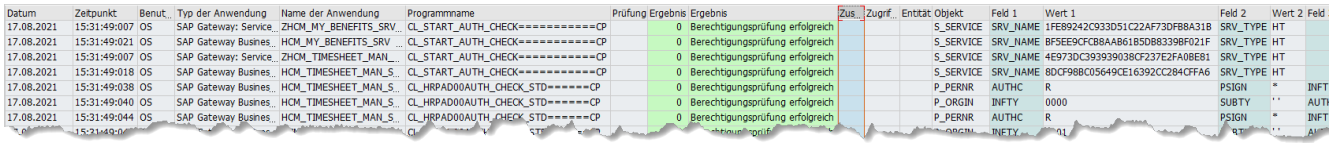


Das Protokoll liefert nun alle Details, welche für eine Zusammenstellung der Details einer Berechtigungsrolle (PFCG -> Berechtigungsobjekte) benötigt werden.



5.4.2. Sonderfall RFC Services

Sofern Fiori Apps und Services aufgerufen und protokolliert werden, so ist im Feldwert nicht der Servicename, sondern die Service-HashID enthalten.

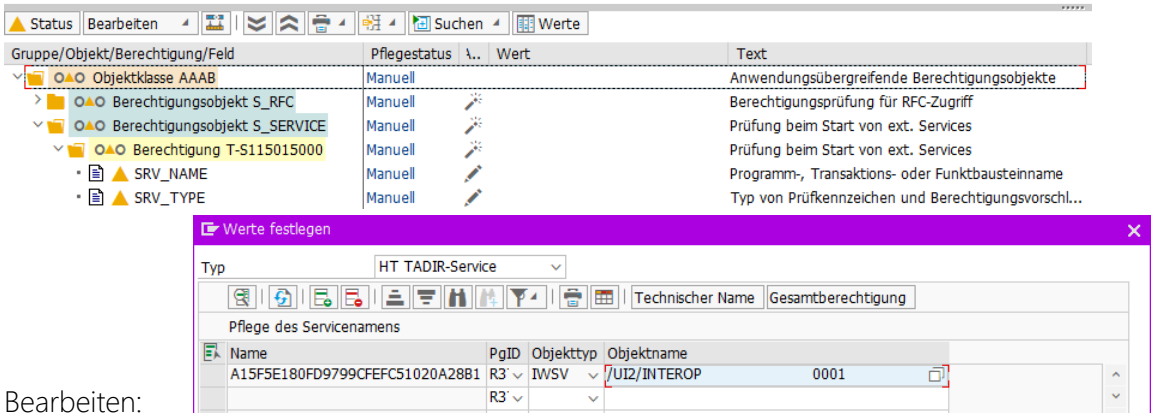


Datum	Zeitpunkt	Benut.	Typ der Anwendung	Name der Anwendung	Programmname	Prüfung Ergebnis	Ergebnis	Zus.	Zugrf.	Entität	Objekt	Feld 1	Wert 1	Feld 2	Wert 2	Feld
17.08.2021	15:31:49:007	OS	SAP Gateway: Service_	ZHCM_MY_BENEFITS_SRV_	CL_START_AUTH_CHECK==========CP	0	Berechtigungsprüfung erfolgreich				S_SERVICE	SRV_NAME	1FE89242C933D51C22AF73DFB8A31B	SRV_TYPE	HT	
17.08.2021	15:31:49:021	OS	SAP Gateway Busines_	HCM_MY_BENEFITS_SRV_	CL_START_AUTH_CHECK==========CP	0	Berechtigungsprüfung erfolgreich				S_SERVICE	SRV_NAME	BF5EE9CFCB8AAB61B5DB8339BF021F	SRV_TYPE	HT	
17.08.2021	15:31:49:007	OS	SAP Gateway: Service_	ZHCM_TIMESHEET_MAN_	CL_START_AUTH_CHECK==========CP	0	Berechtigungsprüfung erfolgreich				S_SERVICE	SRV_NAME	4E973DC393939038CF237E2FA0BE81	SRV_TYPE	HT	
17.08.2021	15:31:49:018	OS	SAP Gateway Busines_	HCM_TIMESHEET_MAN_S_	CL_START_AUTH_CHECK==========CP	0	Berechtigungsprüfung erfolgreich				S_SERVICE	SRV_NAME	8DCF98BC05649CE16392CC284CFFA6	SRV_TYPE	HT	
17.08.2021	15:31:49:038	OS	SAP Gateway Busines_	HCM_TIMESHEET_MAN_S_	CL_HRPAD00AUTH_CHECK_STD======CP	0	Berechtigungsprüfung erfolgreich				P_PERNR	AUTHC	R	PSIGN	*	INFT
17.08.2021	15:31:49:040	OS	SAP Gateway Busines_	HCM_TIMESHEET_MAN_S_	CL_HRPAD00AUTH_CHECK_STD======CP	0	Berechtigungsprüfung erfolgreich				P_ORGIN	INFTY	0000	SUBTY	' '	AUTI
17.08.2021	15:31:49:044	OS	SAP Gateway Busines_	HCM_TIMESHEET_MAN_S_	CL_HRPAD00AUTH_CHECK_STD======CP	0	Berechtigungsprüfung erfolgreich				P_PERNR	AUTHC	R	PSIGN	*	INFT

In Erfassung der Details im Berechtigungsobjekt S_SERVICE muss der Servicename (nicht die HashID) verwendet werden:

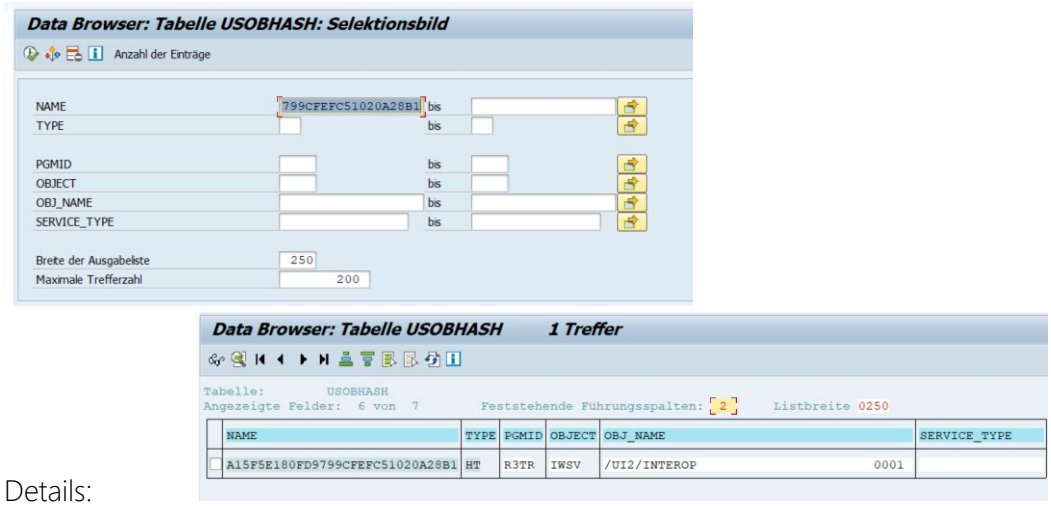
Rolle ZTEST_OS
Pflege: 0 ungepflegte Orgebenen, 24 offene Felder
Status: geändert

Bearbeiten:



Um den Servicenamen anhand der HashID zu finden, können in der Tabelle USOBHASH die Servicedetails (wie z.B. der ServiceName) nachgefragt werden:

Details:



6. Auswertungen Benutzer, Rollen, Berechtigungen, etc.

6.1. Transaktion SUIM Benutzerinformationssystem (Analyse-Cockpit)

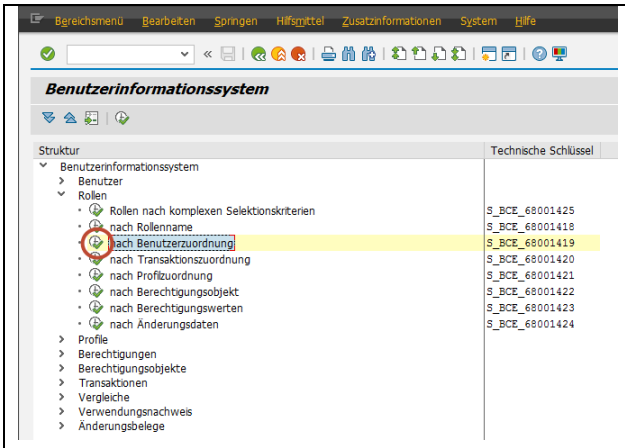
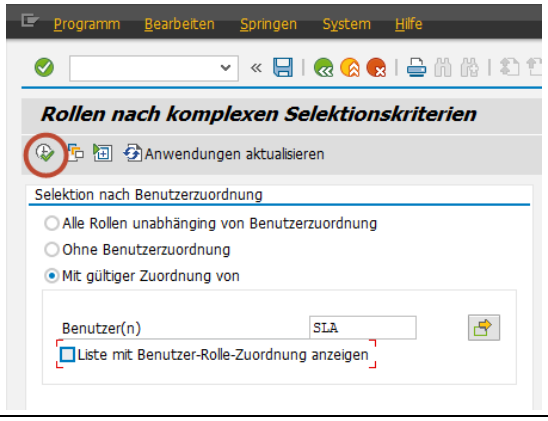
Diese Transaktion bietet z.B. folgende Funktionen (Sammlung von einzelnen, separaten Transaktionen).
► Menü Zusatzinformationen / Anzeige der Transaktionscodes ► blendet Transaktionscodes ein

- Benutzer, Rollen, Profile, Berechtigungen, Berechtigungsobjekte, Transaktionen nach Kriterien auswerten
- Vergleiche von Benutzern, Rollen, Profilen und Berechtigungen
- Verwendungsnachweise für Rollen, Profile, Berechtigungen, Berechtigungswerte, Berechtigungsobjekte und Sicherheitsrichtlinien
- Änderungsbelege auswerten

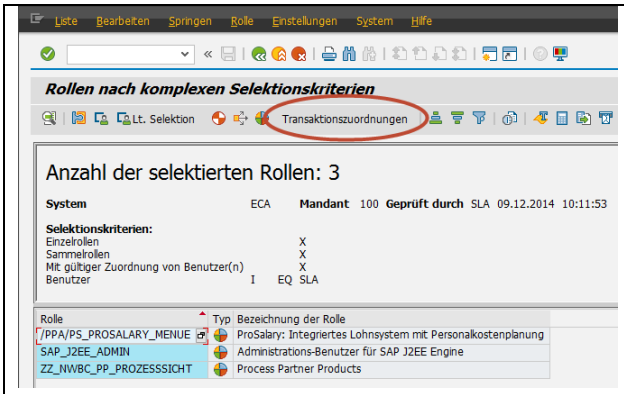
Wir empfehlen, die **Transaktion SUIM** nur wenigen Personen zur Verfügung zu stellen.

6.1.1. Transaktion S_BCE_68001419 Rollen nach Benutzerzuordnung (enthalten in SUIM)

Auswertung	Welche Rollen sind in einer bestimmten Menge von Benutzern enthalten?
Beispiel	Welche Rollen sind in Benutzer SLA enthalten?

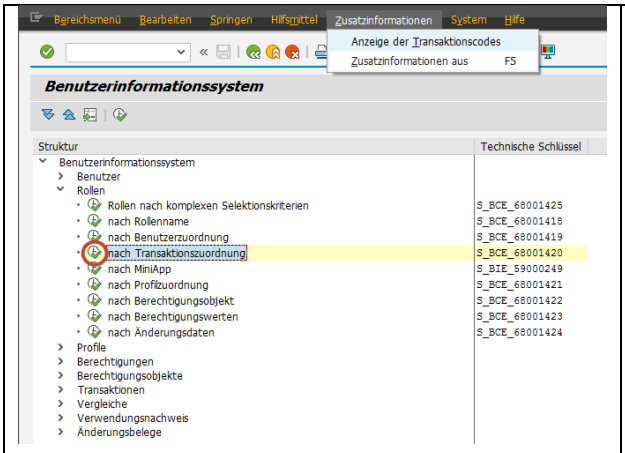
<table>
<tr>
<td> 
</td>
<td>Benutzer eingeben und ausführen
 
</td>
</tr>
<tr>
<td>Ergebnisliste
► markieren einer Rolle
► z.B. Transaktionen dieser Rolle anzeigen

weitere Funktionen pro Rolle
gemäss Drucktastenleiste</td>
<td></td>
</tr>
</table>

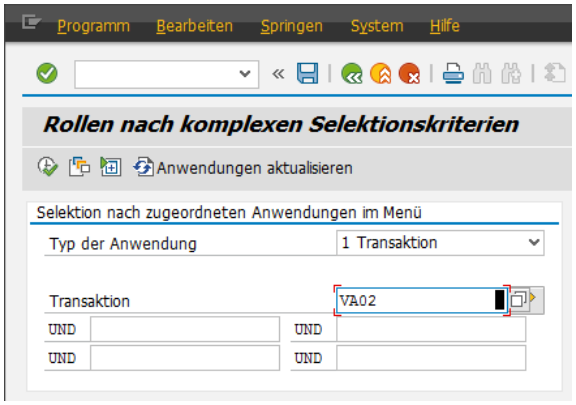


6.1.2. Transaktion S_BCE_68001420 Rollen nach Transaktionszuordnung (enthalten in SUIM)

Auswertung In welchen Rollen sind bestimmte Transaktionen enthalten?
Beispiel In welchen Rollen ist Transaktion VA02 enthalten?

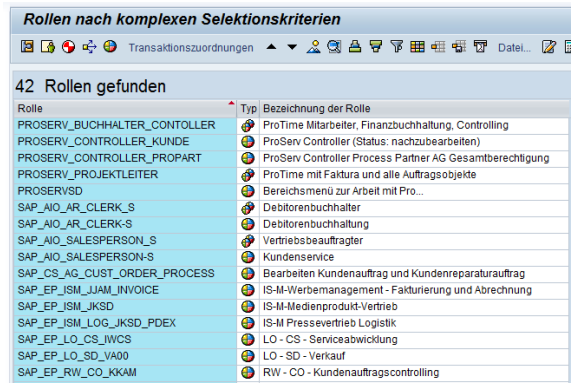


Transaktionscode eingeben und ausführen



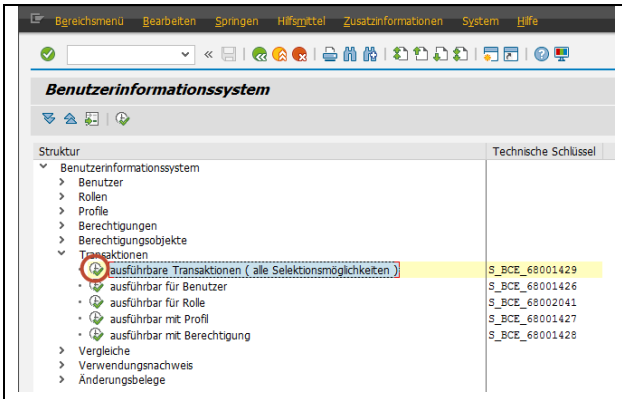
Ergebnisliste

► Doppelklick ► Rolle anzeigen (PFCG)

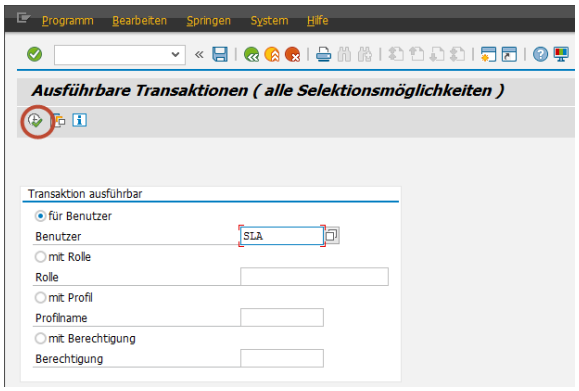


6.1.3. Transaktion S_BCE_68001429 Ausführbare Transaktionen (enthalten in SUIM)

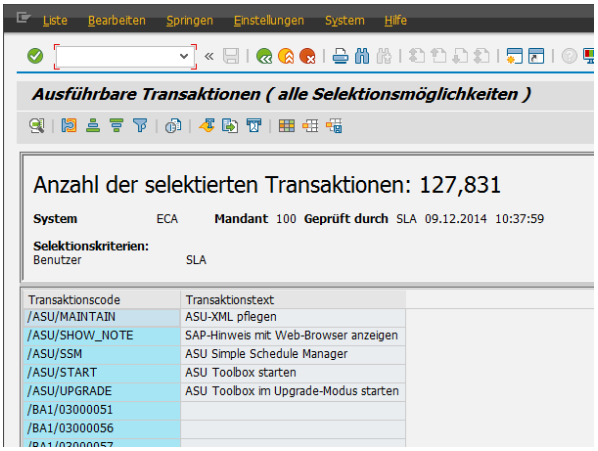
Auswertung Welche Transaktionen kann ein bestimmter Benutzer ausführen?
Beispiel Welche Transaktionen kann Benutzer SLA ausführen?



Benutzer eingeben und ausführen



Ergebnisliste

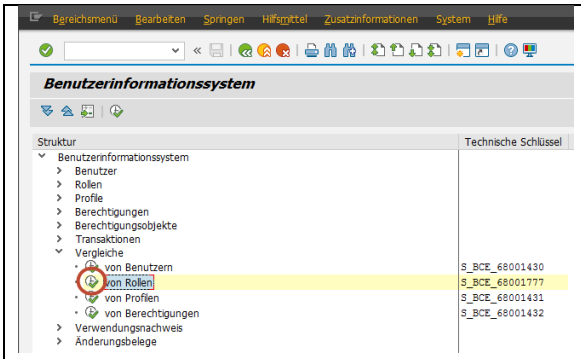


Es werden alle Transaktionen aufgeführt, für die ein Benutzer durch die ihm zugeordneten Rollen berechtigt ist.

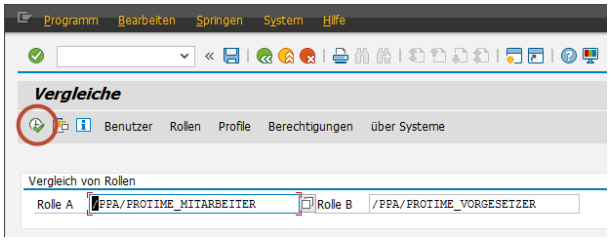
6.1.4. Transaktion S_BCE_68001777 Vergleiche (enthalten in SUIM)

Auswertung Was sind die Unterschiede z. B. zwischen 2 Rollen?

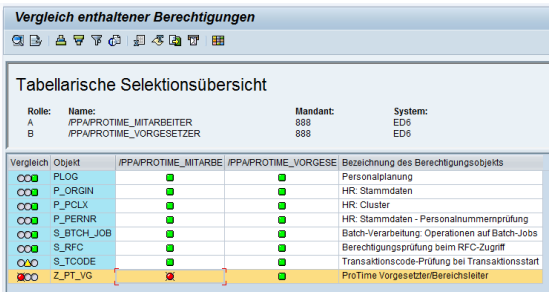
Beispiel Was sind die Unterschiede zwischen Rolle «Mitarbeiter» und «Vorgesetzter»?



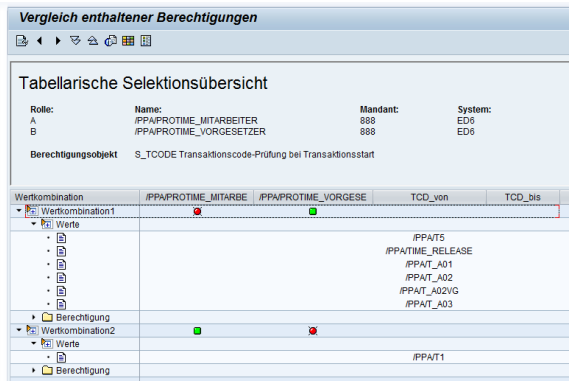
Rollen eingeben und ausführen



Ergebnisliste



Über einen Doppelklick (Zeile S_TCODE) können auch die zugeordneten Transaktionen verglichen werden. Im unteren Beispiel unterscheiden sich die Rollen vollständig. Bei allen anderen Zeilen werden die Ausprägungen der einzelnen Berechtigungsobjekte überprüft.



7. «Lessons learned»

7.1. Grundregeln

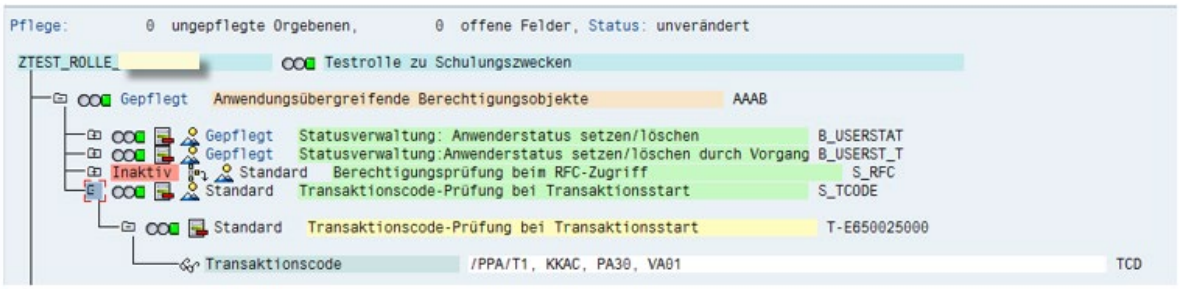
Gehen Sie bei der Ausprägung von Berechtigungsobjekten sorgfältig vor. Deaktivieren Sie etwas «Unbekanntes» lieber, bevor Sie «zu viele» Berechtigungen vergeben. Der Benutzer wird sich melden, wenn er zusätzliche Berechtigungen benötigt.

► Vergeben Sie lieber weniger Berechtigungen als «Überflüssige»

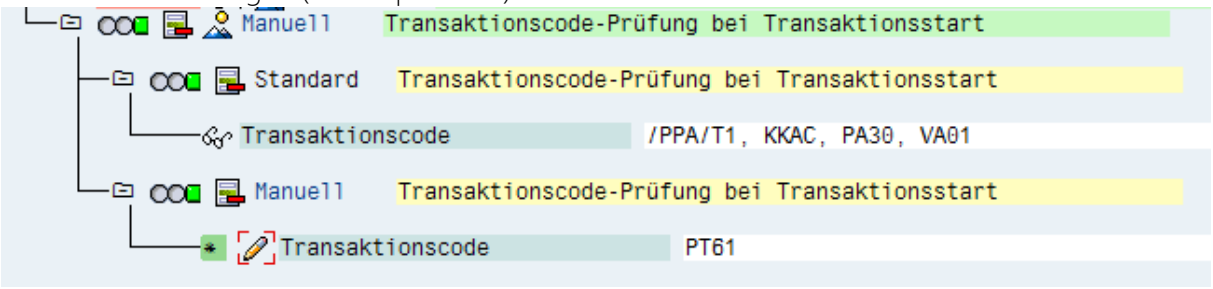
7.2. Zugriff auf Transaktionen im Hintergrund, die nicht in der Menüstruktur erscheinen

Sollte der Benutzer Transaktionen benötigen, die beispielsweise im Hintergrund berechtigt sein müssen, aber nicht im Benutzermenü erscheinen sollen, so können diese Transaktionen im Berechtigungsobjekt

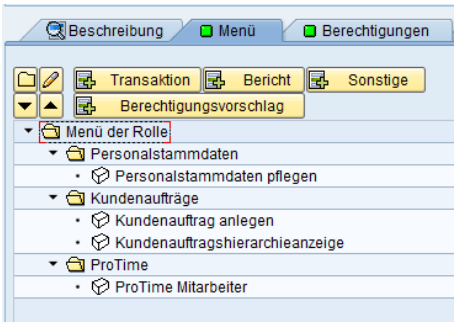
«S_TCODE» auch manuell eintragen.



Sofern das Objekt nicht änderbar ist, können Sie dieses manuell nochmals hinterlegen und weitere Transaktionen eintragen (im Beispiel PT61).



In der Menüstruktur taucht diese Transaktion nicht auf, dennoch ist der Mitarbeiter berechtigt.



7.3. Negativ-Tests

Führen Sie permanent auch «Negativ-Tests» durch, d. h. prüfen Sie nicht nur, ob der Mitarbeiter die Funktionen bearbeiten kann, die er bearbeiten soll.

Prüfen Sie, dass der Mitarbeiter all das nicht aufrufen kann, was er nicht aufrufen soll.