

# Berechtigungen in Fiori

*Fiori-Apps gelten als übersichtlich, leicht zu bedienen und als somit ideal für mobile Endgeräte. Berechtigungen für Fiori funktionieren allerdings anders als bei den ERP-Transaktionen. Ein detailliertes Konzept ist essenziell für den Erfolg einer S/4HANA-Einführung mit Fiori. Zum Start des Projekts reicht es aber völlig aus, mit den von der SAP zur Verfügung gestellten Business-Rollen zu arbeiten, um die Apps schnell kennenzulernen.*



Bildquelle: Adobe Stock/Consilio GmbH

Von Matthias Lebschy\*

**E**s ist kein Geheimnis, dass SAP-Berechtigungen in einem Implementierungsprojekt oft stiefmütterlich behandelt werden. In der Zeit vor Fiori ging man häufig mit einem groben Berechtigungskonzept live, das nach und nach verfeinert wurde. Das lief dann so, dass der Anwender bei einer fehlenden Berechtigung die Transaktion SU53 aufrief und einen Screenshot davon an das Berechtigungsteam schickte.

Das Berechtigungsteam ermittelte auf dem Screenshot das fehlende Berechtigungsobjekt, fügte dieses der Berechtigungsrolle hinzu, und schon konnte der Anwender weiterarbeiten. Das Berechtigungsteam war in den ersten Tagen und Wochen nach dem Go-live stark ausgelastet und die Vorgehensweise war nicht die beste, aber sie hat sich in vielen Projekten bewährt.

Nun wird im Unternehmen Fiori eingeführt, und warum sollte man bei diesen Berechtigungen anders vorgehen als bei ERP-Transaktionen? Wer so denkt, wird schnell bestraft – spätestens beim Go-live. Die Herausforderung bei der Suche nach den fehlenden Berechtigungen in Fiori ist groß, zeitaufwendig und kann meistens nicht so leicht wie gewohnt vom Berechtigungsteam bewältigt werden. Grund dafür ist, dass Screenshots aus der SU53 dem Berechtigungsteam meist nicht mehr helfen, die fehlenden Berechtigungen zu identifizieren.

## **Fiori-Berechtigungen funktionieren anders**

Dies ist der Technologie geschuldet, auf der die Fiori-Anwendung aufbaut. Der Anwender arbeitet mit der Oberfläche, in die er seine Daten eingibt. Das ist das Frontend, das in einem Browser ausgeführt wird. Die Anfrage aus der App wird

an das SAP-System adressiert, denn dort, im Backend-System, befindet sich nach wie vor die Datenbank, die alle Anfragen bearbeitet. Die eingegebenen Daten in der App werden mittels einer Schnittstelle namens „OData“ an das Backend übermittelt. Dafür sind Berechtigungen in Fiori auf verschiedene Ebenen aufgeteilt: Durch die technologischen Gegebenheiten eines Front- (Gateway) und Backend-Systems müssen in beiden Systemen Berechtigungen vergeben werden – sofern kein Embedded Gateway genutzt wird.

Zum einen muss dafür gesorgt werden, dass die relevanten Apps für den User im Fiori-Launchpad nutzbar sind. Dafür werden dem User der Fiori-Katalog und die entsprechende Fiori-Gruppe zugewiesen. Zum anderen muss der User für die Kommunikation zwischen Front- und Backend-System berechtigt und die von der App genutzten OData-Services aktiviert werden.

Fehlen dem Anwender beim Ausführen einer Fiori-App diese Berechtigungen, versagt häufig die Transaktion SU53, denn nicht alle Berechtigungen werden

\*Matthias Lebschy ist Senior Consultant MM / SCM bei Consilio.

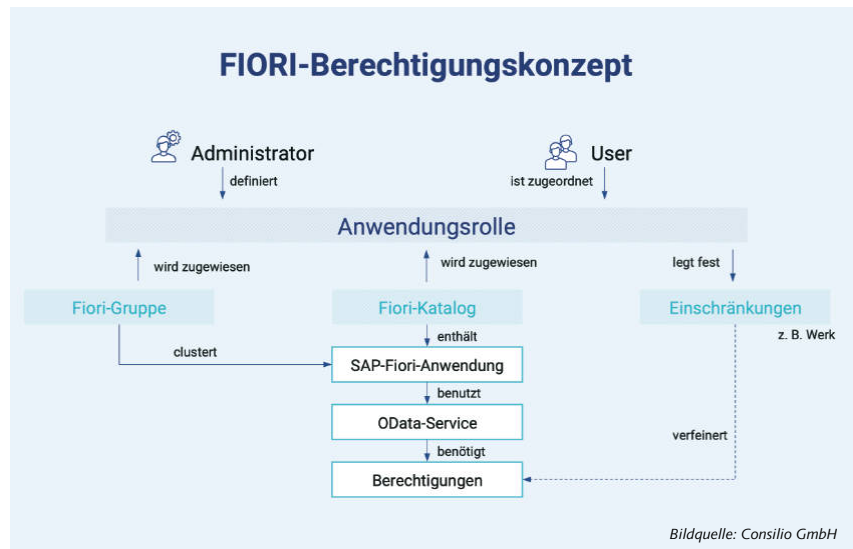
von der SU53 getrackt. Wenn das der Fall ist, greift man zu weiteren Werkzeugen wie Transaktionen N/IWFND/ERROR\_LOG oder /N/IWBEP/ERROR\_LOG. Führt auch das zu keinem Erfolg, kommt man oft am Debuggen nicht vorbei. Dass die Berechtigungsanpassung dann um ein Vielfaches aufwendiger wird, versteht sich von selbst. Multipliziert man den Aufwand mit der Anzahl der Fehler, ergibt sich eine äußerst ungünstige Situation im laufenden Betrieb.

### Wege zu einem soliden Fiori-Berechtigungskonzept

Es gilt also zu vermeiden, dass es im laufenden Betrieb zu aufwendigen Berechtigungsanpassungen kommt. Somit ist ein durchdachtes Berechtigungskonzept für eine erfolgreiche Nutzung von Fiori entscheidend. Die gute Nachricht lautet, dass SAP hier ein hilfreiches Werkzeug entwickelt hat: die Fiori Apps Library. Diese Library ist eine öffentlich zugängliche Sammlung aller Fiori-Applikationen, die zur Verfügung stehen. Neben der Beschreibung der Applikation finden sich dort weitere Informationen, die für Verwendung und Implementierung der App, aber auch für die Erstellung eines Berechtigungskonzepts hilfreich sind:

In die Fiori Apps Library wird ein Suchbegriff eingegeben, beispielsweise „Bestellung anlegen“ oder „ME21N“. Im nächsten Schritt wird eine Trefferliste aller zum Suchbegriff passenden Fiori-Apps angezeigt. Die gesuchte App wird ausgewählt, und unter anderem mit wichtigen Informationen zu den Berechtigungen angezeigt:

- für die App benötigte ICF-Knoten und OData-Services



- benötigte Zielzuordnungen für den Fiori-Katalog
- von der SAP im Standard bereitgestellte Kataloge und ready-to-use Business-Rollen

Wurde eine Business-Rolle identifiziert und gewählt, die im Unternehmen abgebildet werden soll, enthält diese bereits die meisten dafür notwendigen Applikationen. Es empfiehlt sich dabei, nur die tatsächlich benötigten Apps zu aktivieren. Ein Einstieg in die App Library ist des Weiteren über Branchen, Rollen, SAP Best Practices und andere Objekte möglich. Wie die Erfahrung zeigt, ist es, um das Risiko im laufenden Betrieb zu minimieren, lohnend, sich im Vorfeld intensiver mit den Berechtigungen zu beschäftigen.

### Weg über SAP\_ALL-Berechtigung funktioniert nicht

Aber gerade zum Start eines S/4HANA-Projekts möchte man möglichst schnell

einen Einblick in die vorhandenen Fiori-Apps bekommen – auch wenn das Berechtigungskonzept noch nicht erstellt ist. Muss hier von Anfang an das Berechtigungsteam mit eingebunden werden? Oder kann einfach das SAP\_ALL vergeben werden? Beide Fragen können verneint werden. SAP\_ALL-Berechtigung ist zwar die bewährte Lösung in Sandbox-Systemen, um den Berechtigungsproblemen aus dem Weg zu gehen, jedoch werden auch mit SAP\_ALL keine Apps im Launchpad angezeigt. Denn Fiori-Kataloge und Gruppen sind nicht Teil der SAP\_ALL-Berechtigung.

Um nun kein aufwendiges Berechtigungskonzept in der Anfangsphase erstellen zu müssen, können den Usern einfach die Standard-SAP-Business-Rollen zugeordnet werden, die in der Library hinterlegt sind. Damit werden dem User alle Berechtigungen verliehen, um die Apps im Launchpad anzuzeigen und diese auch fehlerfrei auszuführen.

(ch) ©