Benutzerhandbuch

IM.IAM Handbuch

Autor: Chari Lazaridis;Sophie Strecke

Erstelldatum: 27-11-2019

Letzte Änderung: 12-07-2020

Kontrollnummer: OC\_DE/300516442/DO.081/0025

Version: 1.0

**Freigabe:**

|  |  |
| --- | --- |
| Bundeskriminalamt |  |
| Oracle Consulting |  |

logored Kopie-Nr. \_\_\_\_\_

## Dokumentenkontrolle

### Änderungshistorie

| Date | Autor | Version | Änderungsreferenz | |
| --- | --- | --- | --- | --- |
|  |  |  | |  |
| 27-11-19 | Chari Lazaridis | Entwurf | | Kein vorheriges Dokument |
| 06-04-20 | Sophie Strecke | 1.0 | | Anpassungen |
|  |  |  | |  |
|  |  |  | |  |

### Reviewer

| Name | Position |
| --- | --- |
|  |  |
| Rene Donner | Projektleiter |
|  |  |
|  |  |
|  |  |

Inhalt

[Dokumentenkontrolle ii](#_Toc45467292)

[Änderungshistorie ii](#_Toc45467293)

[Reviewer ii](#_Toc45467294)

[Einführung 1](#_Toc45467295)

[eFBS Teilnehmer 1](#_Toc45467296)

[Typografische Konventionen 1](#_Toc45467297)

[Hintergrund und Zielbild 2](#_Toc45467298)

[Grundlagen 2](#_Toc45467299)

[Namenskonventionen 2](#_Toc45467300)

[CR2131 – Admin-Benutzer in eFBS 2](#_Toc45467301)

[Zielbild 3](#_Toc45467302)

[Endanwender 3](#_Toc45467303)

[Anmeldung 5](#_Toc45467304)

[Kennwort und Zugriffsberechtigung 5](#_Toc45467305)

[Kennwort und Erstzugriff 5](#_Toc45467306)

[Zugriffsberechtigungen 5](#_Toc45467307)

[Verwalten von Identitäten 6](#_Toc45467308)

[Identitäten suchen 6](#_Toc45467309)

[Einfache Suche 7](#_Toc45467310)

[Erweiterte Suche 7](#_Toc45467311)

[Identitäten anzeigen 8](#_Toc45467312)

[Identitäten manuell erfassen 9](#_Toc45467313)

[Anforderungsinformationen 10](#_Toc45467314)

[Basisinformation 10](#_Toc45467315)

[Accounteinstellungen 11](#_Toc45467316)

[Daten für Accountgültigkeit 12](#_Toc45467317)

[Attribute Kontaktinformationen 12](#_Toc45467318)

[Identität manuell ändern 13](#_Toc45467319)

[Kennwort rücksetzen 13](#_Toc45467320)

[Deaktivieren/Aktivieren der Identität 15](#_Toc45467321)

[Sperren/Entsperren der Identität 17](#_Toc45467322)

[Ändern von Attributen 20](#_Toc45467323)

[Vergabe eFBS Fachanwenderrolle 21](#_Toc45467324)

[Auswahl der Identitäten 21](#_Toc45467325)

[Auswahl der Rolle 21](#_Toc45467326)

[Anfordern 22](#_Toc45467327)

[Initiale Anlage von Speziellen eFBS Benutzerkonten 23](#_Toc45467328)

[Prüfpunkt und Aufruf des Katalogs 23](#_Toc45467329)

[Aktualisieren der Warenkorbelemente 24](#_Toc45467330)

[eFBS Application Account für fa, su, gfa, gsu 24](#_Toc45467331)

[eFBS Citrix Terminal Services fa, su, gfa, gsu 26](#_Toc45467332)

[Weiterleitung und Abschluss 29](#_Toc45467333)

[Kennwortadministration 30](#_Toc45467334)

[Setzten des Kennwortes für eFBS Systemaccounts 30](#_Toc45467335)

[Setzten des Kennwortes für Administrationskonten 31](#_Toc45467336)

[Ausnahmesituation: Verwendung der „Gemeinsamen Ermittlerdatei (GED)“ 33](#_Toc45467337)

## Einführung

### eFBS Teilnehmer

Nachfolgendes Dokument richtet sich an alle Teilnehmer, die am neuen eFBS Verfahren partizipieren. Es werden grundlegende Operationen im Rahmen von Identity und Access Management erläutert. Diese betreffen in erster Linie die Länderadministratoren und nicht jeden eFBS Endanwender.

Folgende Themen/ Operationen werden erläutert:

* Anmeldung am Identity Manager
* Vergabe eFBS Fachanwenderrolle
* Initiale Anlage von Speziellen eFBS Benutzerkonten
  + Globale Fachadministratoren
  + Globale Superadministratoren
  + Fachadministratoren
  + Superadministratoren
* Verwendung von Sonderaccounts in eFBS
  + rssuper
  + property\_user
  + property\_user\_glob
* Ausnahmesituation: Verwendung der „Gemeinsamen Ermittlerdatei (GED)“

### Typografische Konventionen

Die folgenden typografischen Konventionen werden in diesem Dokument verwendet.

|  |  |
| --- | --- |
| **Konvention** | **Bedeutung** |
| **Fettdruck** | Fettdruck kennzeichnet Elemente der grafischen Benutzeroberfläche, die einer Aktion zugeordnet sind, oder Begriffe, die im Text oder im Glossar definiert sind. |
| *kursiv* | Kursivschrift kennzeichnet Buchtitel, Hervorhebungen oder Platzhalter, für die Sie bestimmte Werte angeben. |
| monospace | Monospace kennzeichnet in einem Absatz Befehle, URLs, Code-Beispiele, Text, der auf dem Bildschirm angezeigt wird, oder Text, den Sie eingeben.. |

## Hintergrund und Zielbild

### Grundlagen

#### Namenskonventionen

Gemäß CR 2131 wird auch den Benutzern des Bundeskriminalamts das TN-Kürzel „BK“ vorangestellt. Daher müssen sie in der gleichen Weise migriert werden die Benutzer der Bundespolizei (vorangestelltes Kürzel „BP“).

Beispiel: bk4711123 wird zu BK4711123

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Bei der Anmeldung am Fachverfahren eFBS (nur relevant in Umgebungen, die kein IAM haben) kann der Benutzername in Kleinbuchstaben eingegeben werden, auch wenn er tatsächlich Großbuchstaben enthält. |

#### CR2131 – Admin-Benutzer in eFBS

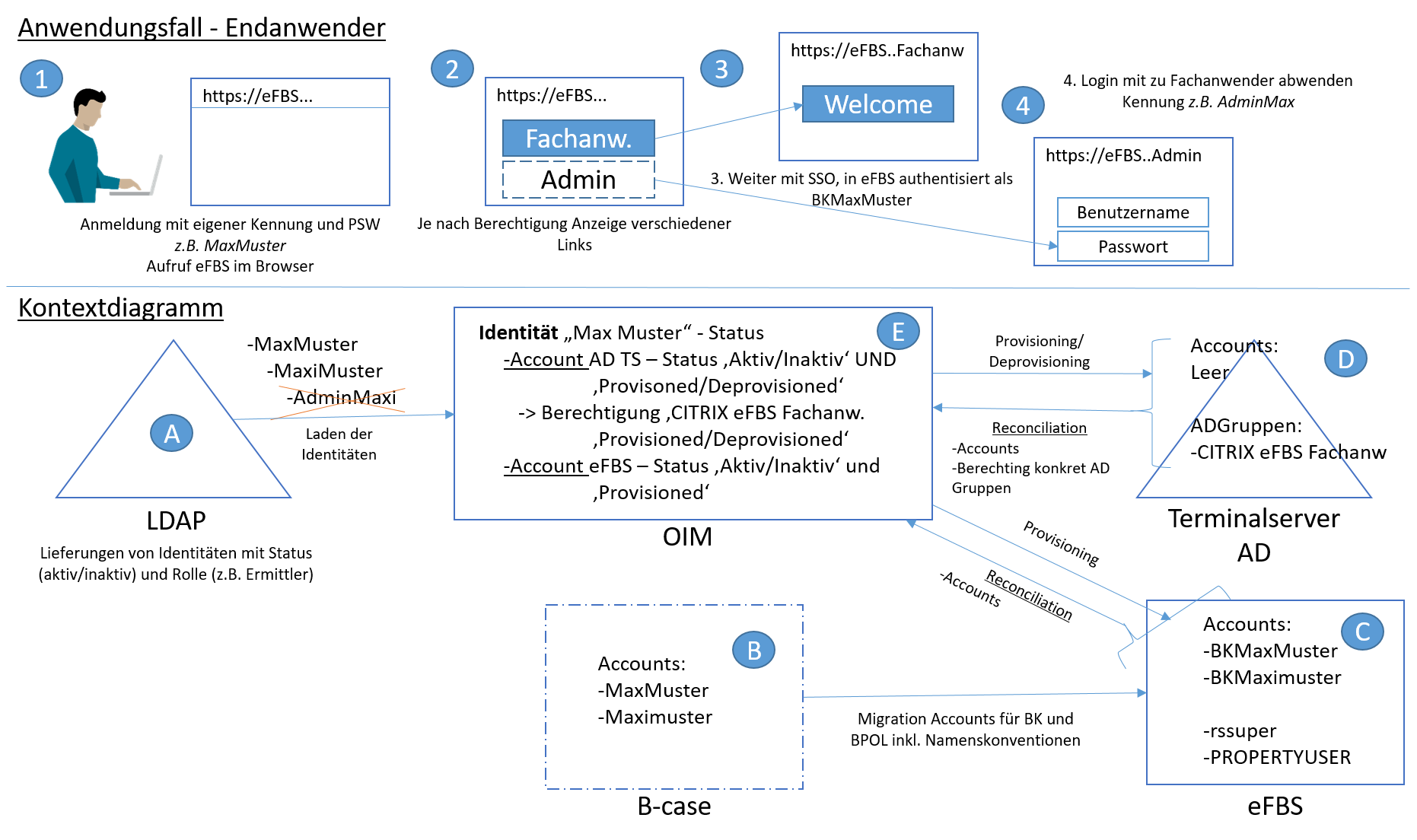
Alle Identitäten der eFBS-Fachanwendungs-Benutzer werden von den TN-Systemen an IAM mitgeteilt, die TN-Systeme sind führend. Eine solche Identität kann im Identity Manager verschiedene Benutzerkonten auf einem oder verschiedenen IT-Systemen haben und diese wiederum haben Berechtigungen, z.B. für die Fachanwendung und die Admin-Anwendungen. Diese Benutzerkonten (= Accounts) werden aus dem IAM per SCIM-Schnittstelle mit eFBS synchronisiert. Sie heißen <TN><Benutzername >, z.B. BWLindeNor. Die Anmeldung am Fachverfahren eFBS erfolgt über Single Sign On.

| **Namensteil** | **Bedeutung** |
| --- | --- |
| **TN** | Kennung des Teilnehmers  Beispiel: BW |
| **Benutzername** | Name des Benutzers in der Datenquelle des Teilnehmers  Beispiel: LindeNor |

Die Benutzernamen wurden im Identity Manager bereits mit vorangestelltem TN-Kürzel angelegt.

|  | **Achtung** |
| --- | --- |
| Die eFBS-Admin-Benutzer werden im Identity Manager als **zusätzliche Benutzerkonten zum bereits bestehenden eFBS Benutzerkonto** unterhalb einer Identität (natürliche, atmende Person) von den TN angelegt und bezüglich der Kennwörter verwaltet. |

### Zielbild



#### Endanwender

Der Endanwender soll mit dem Go-Live von eFBS:

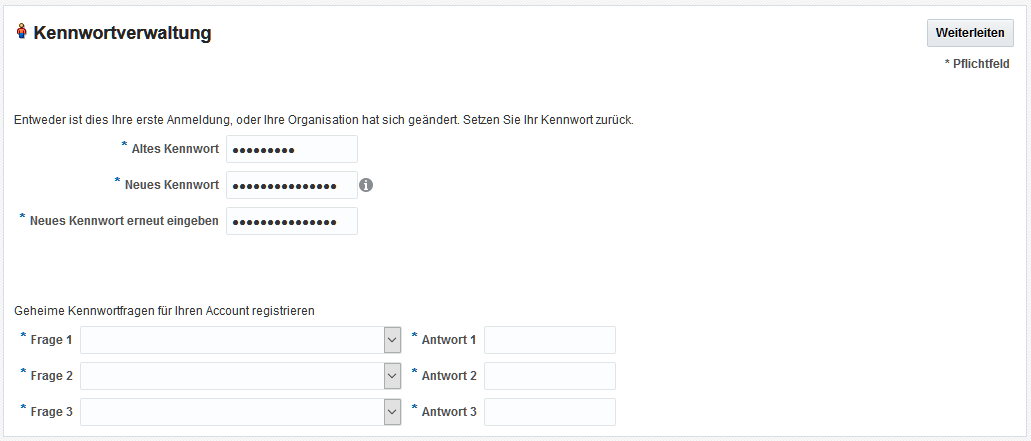
1. Sich mit seiner ihm bekannten Kennung/seinem Kennwort anmelden und durch eine URL im Browser eine CITRIX Terminal-Server-Session aufrufen
2. Abhängig von seinen Berechtigungen in der Active Directory (AD) der Terminal-Server-Umgebung erscheinen Links innerhalb der Terminal-Server-Session z.B. „eFBS Fachanwender“ oder „eFBS Admin“
3. Fachanwender gelangen über Single Sign On zur eFBS-Fachanwendung. Hier ist der Nutzer mit der bereits umgewandelten Kennung (inkl. Teilnehmer-kürzel) authentisiert
4. Für Administratoren wird kein Single-Sign-On-Verfahren durchgeführt. Beim Klick auf eine Administratoranwendung wird der Benutzer nach Benutzerkonto/Kennwort abgefragt.
5. Alle Teilnehmer stellen über eine Datenquelle (LDAP) Identitäten inkl. deren Status und einer Businessrolle zur Verfügung. Innerhalb dieser Datenquelle dürfen keine Identitäten mit unterschiedlichen Kennungen (z.B. MaxMuster und AdminMax) auftauchen. Vor der Migration müssen alle Teilnehmer in ihrem AD /BV die Identitäten anlegen.
6. Da eFBS in einer Terminal-Server-Umgebung läuft, ist für die Realisierung des Zugriffs ein MS AD nötig, hier als Terminal-Server AD bezeichnet. Um auf die verschiedenen Anwendungskomponenten (z.B. für Fachanwender, Admin) zugreifen zu können, sind zusätzlich zum AD TS Account AD Gruppenmitgliedschaften nötig. Jeder Link auf eine Anwendungskomponente stellt dabei eine eigene AD Gruppe dar.
7. OIM liest Identitäten aus der Datenquelle eines Teilnehmers (A) Identitäten und deren Status (aktiv/inaktiv) aus. Für jeden Eintrag in der Datenquelle wird ein Eintrag im OIM generiert und der Status übernommen. Die Datenquelle eines Teilnehmers ist stets der Master dieser Einträge. OIM besitzt keine Schreibrechte in der Datenquelle eines Teilnehmers.
8. Weiterhin werden durch Verfahren zum Datenabgleich vorhandene eFBS-Accounts durch heuristische Regelwerke (Matching Rules) mit der Identität verknüpft. Weitere Berechtigungen werden manuell durch die Benutzerverwaltung in eFBS gesetzt (Limitierung durch die Schnittstelle).
9. Für das Terminal-Server AD (C) werden zunächst die vorhandenen AD Gruppen abgeglichen, d.h. die Menge an AD Gruppen, welche durch das AD bereitgestellt wird, ohne dass diese einem oder mehreren Nutzern zugewiesen sein müssen. TS AD Accounts sind nach dem Zeitpunkt der Bereitstellung keine vorhanden.

## Anmeldung

### Kennwort und Zugriffsberechtigung

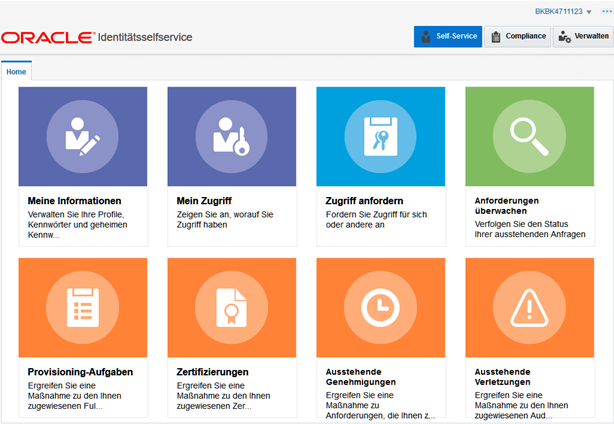
#### Kennwort und Erstzugriff

Sie erhalten Ihr Kennwort vom Systembetrieb. Bei der ersten Anmeldung werden Sie durch die Kennwortverwaltung aufgefordert, ein neues Kennwort zu setzen.



In der Kennwortverwaltung beantworten Sie ebenfalls die durch Sie auszuwählenden Kennwortfragen.

#### Zugriffsberechtigungen



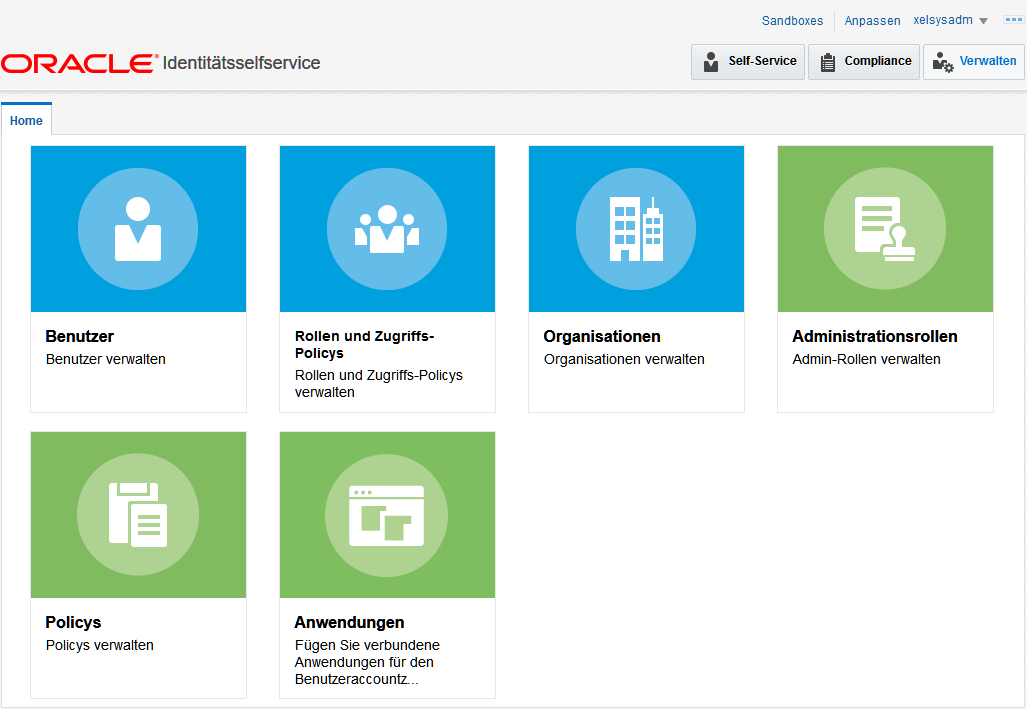
Diese Berechtigungen werden bestimmten Identitäten zugewiesen, damit diese, wie z.B. die Kennwortadministratoren, Benutzerkonten anderer Identitäten manipulieren können. Im Falle eines Kennwortadministrators wäre das z.B. das Rücksetzen des Kennworts für die Benutzerkonten.

## Verwalten von Identitäten

|  | **Achtung** |
| --- | --- |
| Das Anlegen von Identitäten wird über Berechtigungen gesteuert.  Für die Teilnehmer Baden-Württemberg, Brandenburg, , Hamburg, Hessen, das Bundeskriminalamt und die Bundespolizei, ist das nachfolgend beschriebene Vorgehen nicht anwendbar. |

Vergewissern Sie sich zuvor, ob Sie die entsprechenden Berechtigungen zum Anlegen von Identitäten besitzen. Im Kapitel eFBS Teilnehmer ist beschrieben welche Berechtigungen Sie dafür benötigen.

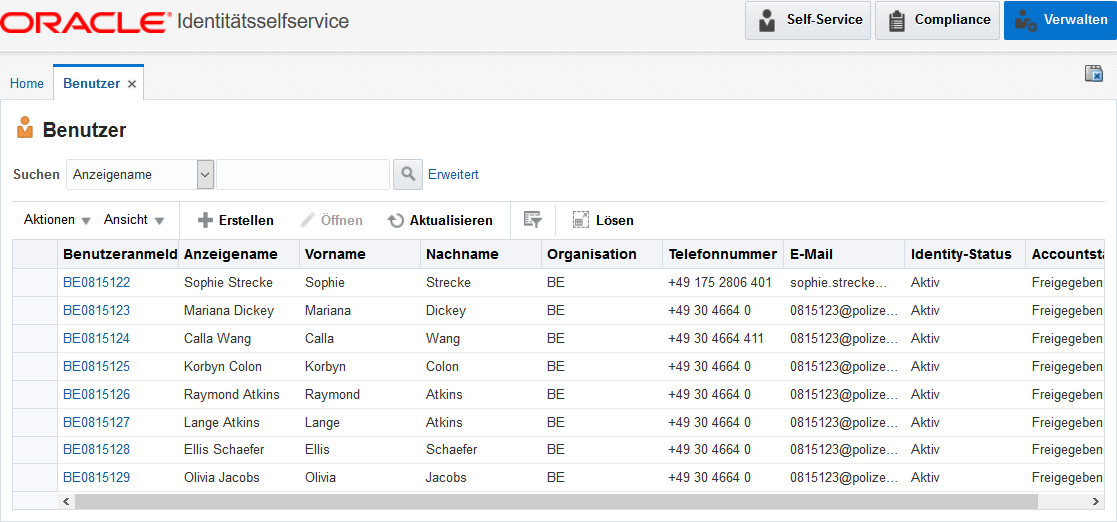
Wählen Sie globalen den Navigationsbereich **Verwalten** und danach **Benutzer** aus.



2

1

Sie gelangen in die Ansicht der administrierbaren Identitäten. Die Ansicht basiert auf Ihrer Teilnehmerkennung und damit verbundenen Berechtigung.



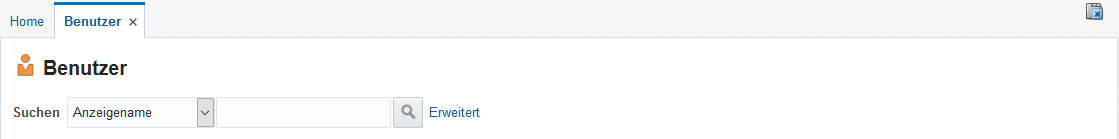
### Identitäten suchen

Mit dem Suchvorgang können Sie Identitäten anhand der von Ihnen angegebenen Suchkriterien durchsuchen. Jedes Suchkriterium besteht aus:

* Das Attribut, nach dem gesucht werden soll
* Die Suchoperatoren, z. B. Gleich und Beginnt mit
* Die zu suchenden Werte.

Verwenden Sie die Seite Benutzer, um eine einfache oder erweiterte Suche nach Identitäten durchzuführen.

#### Einfache Suche



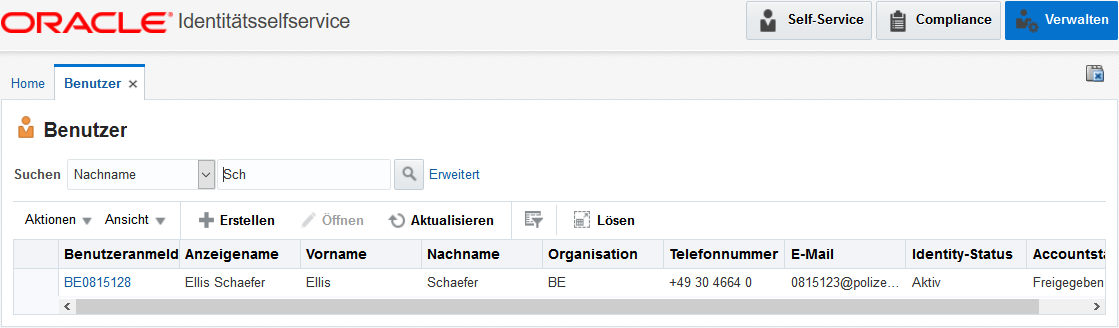
In der Dropdown-Liste **Suchen** stehen Ihnen folgende Attribute nach denen gesucht werden kann zur Verfügung

* Anzeigename
* Benutzeranmeldung
* Vorname
* Nachname
* E-Mail
* Organisation
* Identity-Status
* Accountstatus
* Startdatum
* Enddatum

Um eine einfache Suche durchzuführen, wählen Sie eines dieser Attribute und geben in dem Freitextfeld einen Suchbegriff ein.

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Der Suchoperation in diesem Modus ist **Beginnt mit** für Textfelder.  Für Status‑ und Datumsfelder wird der Operator **Gleich** angewendet. |

Klicken Sie auf das Suchsymbol.

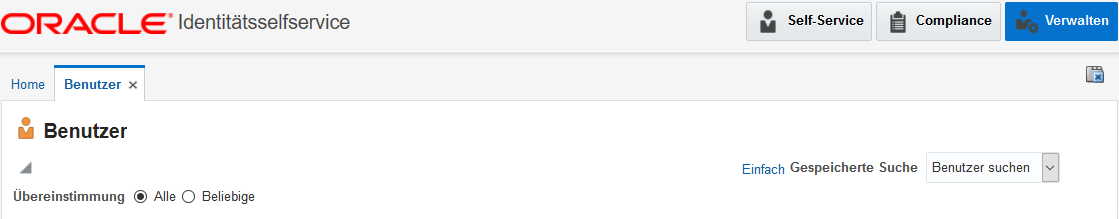


In der Ergebnisliste erscheinen tabellarisch Identitäten die zu dem ausgewählten Suchkriterium passen.

|  | **Achtung** |
| --- | --- |
| Das Suchergebnis beinhaltet ausschließlich Identitäten für die Sie berechtigt sind.  Identitäten außerhalb dieser Zuständigkeit werden Ihnen nicht angezeigt. |

#### Erweiterte Suche

In der erweiterten Suche legen Sie zunächst fest, wie die Kombinatorik der einzelnen Suchkriterien gestaltet werden soll.



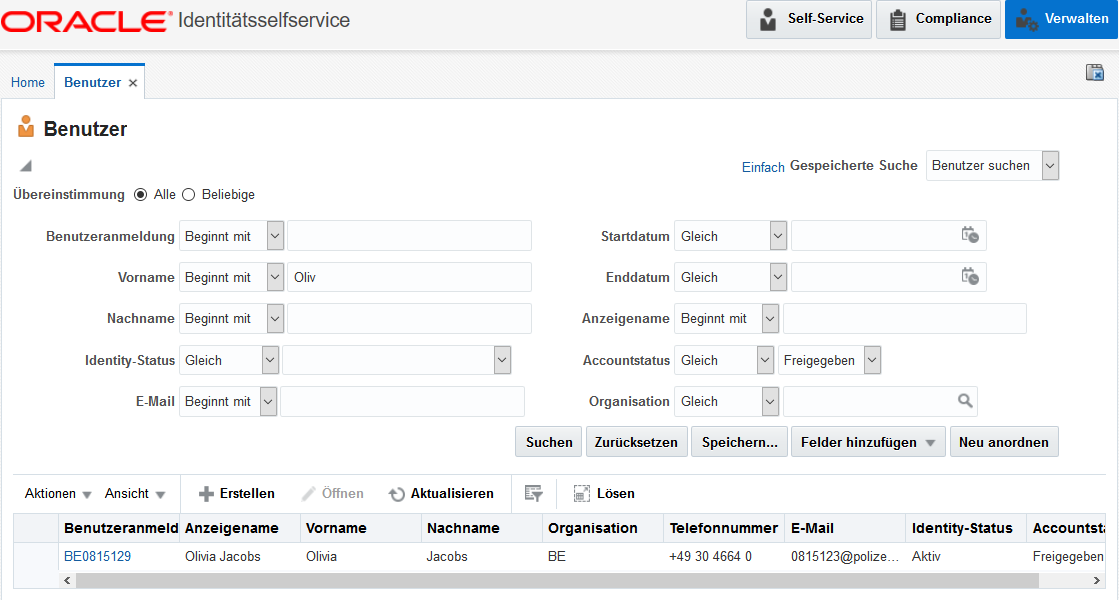
| **Übereinstimmung** | **Verhalten** |
| --- | --- |
| **Alle** | Bei Auswahl dieser Option wird die Suche mit der UND-Bedingung durchgeführt. Dies bedeutet, dass der Suchvorgang nur dann erfolgreich ist, wenn alle angegebenen Suchkriterien übereinstimmen. |
| **Beliebig** | Bei Auswahl dieser Option wird die Suche mit der ODER-Bedingung durchgeführt. Dies bedeutet, dass der Suchvorgang erfolgreich ist, wenn ein angegebenes Suchkriterium übereinstimmt. |

Geben Sie in den durchsuchbaren Benutzerattributfeldern, z. B. Benutzeranmeldung, einen Wert an. Sie können Platzhalter (\*) in den Attributwert aufnehmen.

Für einige Attribute können Sie den Attributwert aus einer Liste auswählen. Um beispielsweise alle Benutzer mit gesperrten Konten zu durchsuchen, wählen Sie in der Liste **Accountstatus** die Option **Gesperrt** aus.

Wählen Sie für jeden von Ihnen angegebenen Attributwert einen Suchoperator aus der zur Verfügung stehenden Liste aus. Die Suchoperatoren variieren dabei nach Attributtyp.

Klicken Sie auf die Schaltfläche **Suchen**.



3

2

1

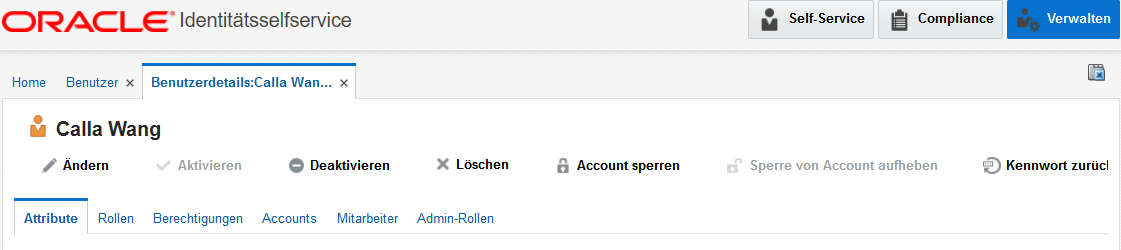
In der Ergebnisliste erscheinen tabellarisch Identitäten die zu den ausgewählten Suchkriterien passen.

|  | **Achtung** |
| --- | --- |
| Das Suchergebnis beinhaltet ausschließlich Identitäten für die Sie berechtigt sind.  Identitäten außerhalb dieser Zuständigkeit werden Ihnen nicht angezeigt. |

### Identitäten anzeigen

Mit der Schaltfläche **Öffnen** können Sie detaillierte Profilinformationen einer Identität auf der Seite **Benutzerdetails** anzeigen.

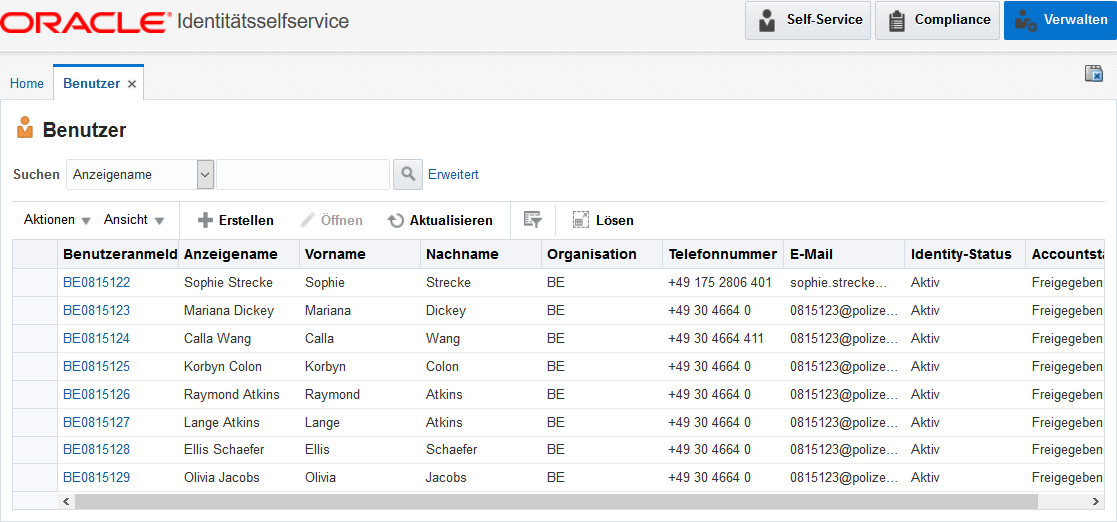
Sie können diese Seite öffnen, wenn Sie berechtigt sind, das Profil einer Identität gemäß der vergebenen Berechtigungsrichtlinie anzuzeigen.



| **Registerkarte** | **Verhalten** |
| --- | --- |
| **Attribute** | Zeigt das Attributprofil an, das Details zu grundlegenden Informationen der Identität, Gültigkeitsdaten des Kontos und Bereitstellungsdaten enthält. Weitere Informationen finden Sie unter Ändern von Attributen im Abschnitt Identität manuell ändern. |
| **Rollen** | Zeigt eine Liste der Rollen an, zu denen die Identität gehört. Sie können auf jede Rolle klicken, um zusammenfassende Informationen zur Rolle anzuzeigen.  Auf der Registerkarte Rollen können Sie der Identität Rollen zuweisen und Rollen der Identität entziehen. Weitere Informationen finden Sie unter Vergabe eFBS Fachanwenderrolle. |
| **Berechtigungen** | Zeigt eine Liste der Berechtigungen für die Identität an. Sie können auf jede Berechtigung klicken, um eine Zusammenfassung der Berechtigung anzuzeigen.  Auf der Registerkarte Berechtigungen können Sie Berechtigungen anfordern und Berechtigungen von der Identität entfernen. |
| **Accounts** | Zeigt eine Liste der Konten für die Identität an. Sie können auf jedes Konto klicken, um eine Zusammenfassung des Kontos anzuzeigen.  Typische Aufgaben, die Sie auf dieser Registerkarte ausführen, sind das Anfordern eines Kontos, das Ändern und Entfernen von Konten, das Markieren eines Kontos als primär sowie das Deaktivieren und Aktivieren von Konten. Weitere Informationen finden Sie unter Initiale Anlage von Speziellen eFBS Benutzerkonten. |
| **Mitarbeiter** | Zeigt eine schreibgeschützte Tabelle der Identitäten an, für die die Identität als Manager festgelegt ist. Mit anderen Worten, diese Registerkarte listet die direkt Unterstellten der Identität auf. |
| **Admin Rollen** | Zeigt eine Liste der der Identität zugewiesenen Administratorrollen an. Sie können eine Administratorrolle auswählen, um eine Zusammenfassung der Administratorrolle anzuzeigen. |

### Identitäten manuell erfassen

Für das erfassen einer neuen Identität verwenden Sie die Schaltfläche **Erstellen**.

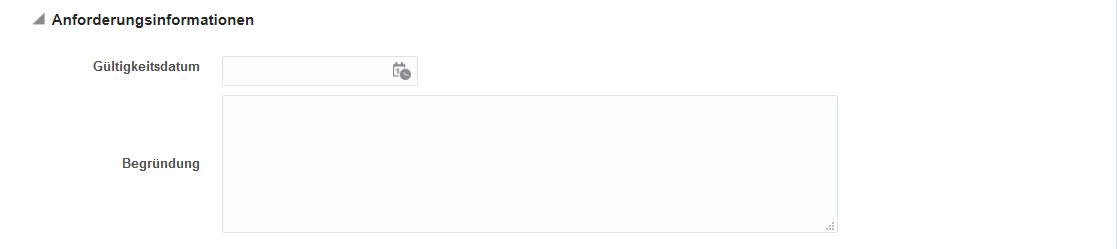


Dadurch wird der Vorgang zur Erstellung einer Identität geöffnet.

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Identity Manager ist derart konfiguriert, dass keine nachgelagerte Genehmigung zur Erstellung der Identität eingeholt wird. |

|  | **Achtung** |
| --- | --- |
| Einige Attribute einer Identität sind erforderlich. Diese Attribute sind mit einem Stern als Symbol gekennzeichnet.  Ohne eine Eingabe in diesen Attributen kann der Vorgang nicht abgeschlossen werden. |

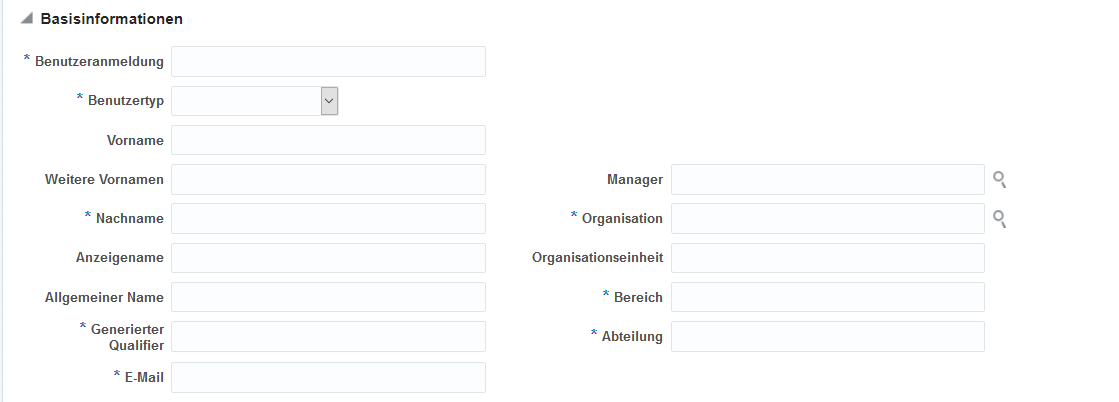
#### Anforderungsinformationen



Die Anforderungsinformationen erfassen den Zeitpunkt wann der Vorgang eintreten soll und die Begründung weshalb der Vorgang ausgelöst wird.

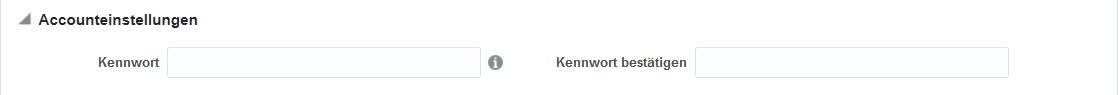
| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Diese Daten sind für das Anlegen einer Identität nicht erforderlich und sollten frei bleiben |

#### Basisinformation



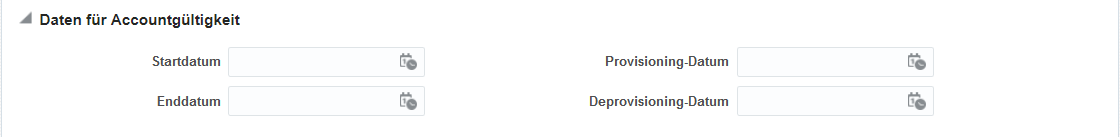
| **Attribute** | **Bedeutung** |
| --- | --- |
| **Benutzeranmeldung** | Der Anmeldename der Identität.  Dieser Name wird auch für die Anmeldung an den zentral bereitgestellten Fachverfahren verwendet. |
| **Benutzertyp** | Der Typ der Identität im System. |
| **Vorname** | Der Vorname des Identität. |
| **Weitere Vornamen** | Die weiteren Vornamen der Identität |
| **Nachname** | Der Nachname der Identität.  Dies ist ein Pflichtfeld. |
| **Anzeigename** | Der Anzeigename der Identität.  Wenn nicht angegeben, wird dieser Name beim Erstellen der Identität automatisch generiert. |
| **Allgemeiner Name** | Der allgemeine Name der Identität.  Wenn nicht angegeben, wird dieser Name beim Erstellen der Identität automatisch generiert. |
| **Generierter Qualifier** | Das Qualifizierungsmerkmal der Identität im Verbund.  Dieser Name ist der teilnehmerspezifische User Principal Name, mit dem sich ein Benutzer bei einem lokal bereitgestellten Fachverfahren anmeldet.  Die Herkunft und Ausprägung dieses Attributs wir zumeist durch das Micosoft Active Directory eines Teilnehmers bestimmt. |
| **E-Mail** | Die E-Mail-Adresse der Identität.  Dies ist ein Pflichtfeld. |
| **Identity Status** |  |
| **Accountstatus** | Gibt an, ob das Benutzerkonto der Identität im Identity Manager gesperrt oder entsperrt ist. |
| **Manager** |  |
| **Organisation** |  |
| **Organisationseinheit** |  |
| **Bereich** |  |
| **Abteilung** |  |

#### Accounteinstellungen



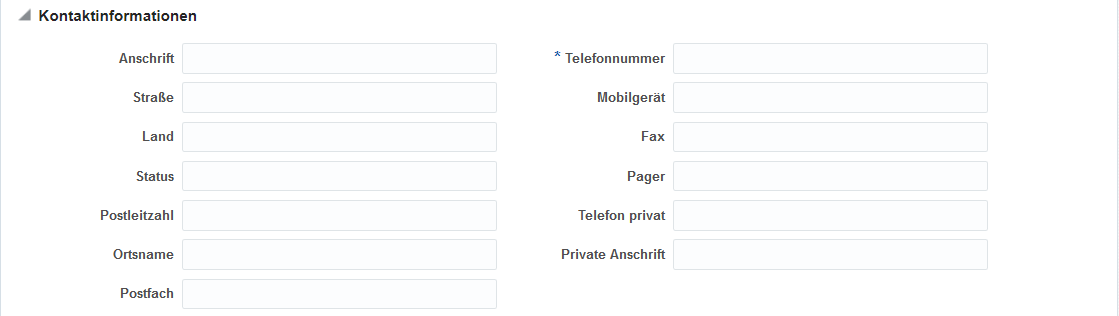
| **Attribute** | **Bedeutung** |
| --- | --- |
| **Kennwort** | Das Kennwort der Identität, das für die Anmeldung an der Self-Service Konsole verwendet werden soll.  Wenn nicht angegeben, wird ein Kennwort beim Erstellen der Identität automatisch generiert.  Es wird als verschlüsselter Wert gespeichert. |
| **Kennwort bestätigen** | Bestätigung des Kennworts, falls eines eingegeben wurde |

#### Daten für Accountgültigkeit



| **Attribute** | **Bedeutung** |
| --- | --- |
| **Startdatum** | Das Startdatum der Identität. |
| **Enddatum** | Das Enddatum der Identität. |
| **Provisioning-Datum** | Das Datum, an dem das Profil der Identität in Identity Manager erstellt wurde. |
| **Deprovisioning-Datum** | Das Datum, an dem die der Identität zugewiesenen Ressourcen freigegeben werden. |

#### Attribute Kontaktinformationen



| **Attribute** | **Bedeutung** |
| --- | --- |
| **Anschrift** | Die dienstliche Postanschrift der Identität.  Thaerstr. 11, Wiesbaden |
| **Straße** | Der Straßenname einschließlich Hausnummer des Dienstsitzes der Identität  Beispiel: Thaerstr. 11 |
| **Land** | Das Land des Dienstsitzes der Identität.  Beispiel: Deutschland |
| **Postleitzahl** | Die Postleitzahl des Dienstsitzes der Identität, falls vorhanden.  Beispiel: Deutschland |
| **Ortsname** | Der Name des Ortes des Dienstsitzes der Identität, falls vorhanden.  Beispiel: Wiesbaden |
| **Postfach** | Das Postfach des Dienstsitzes der Identität, falls vorhanden. |
| **Telefonnummer** | Die dienstliche Telefonnummer der Identität.  Dies ist ein Pflichtfeld. |
| **Mobilgerät** | Die Nummer eines mobilen Endgeräts, dass die Identität verwendet. |
| **Fax** | Die dienstliche Telefaxnummer der Identität. |
| **Pager** | Die dienstliche Nummer des Pagers der Identität, falls vorhanden. |
| **Telefon Privat** | Die private Telefonnummer der Identität, falls vorhanden. |
| **Private Anschrift** | Die private Postanschrift der Identität, falls vorhanden. |

### Identität manuell ändern

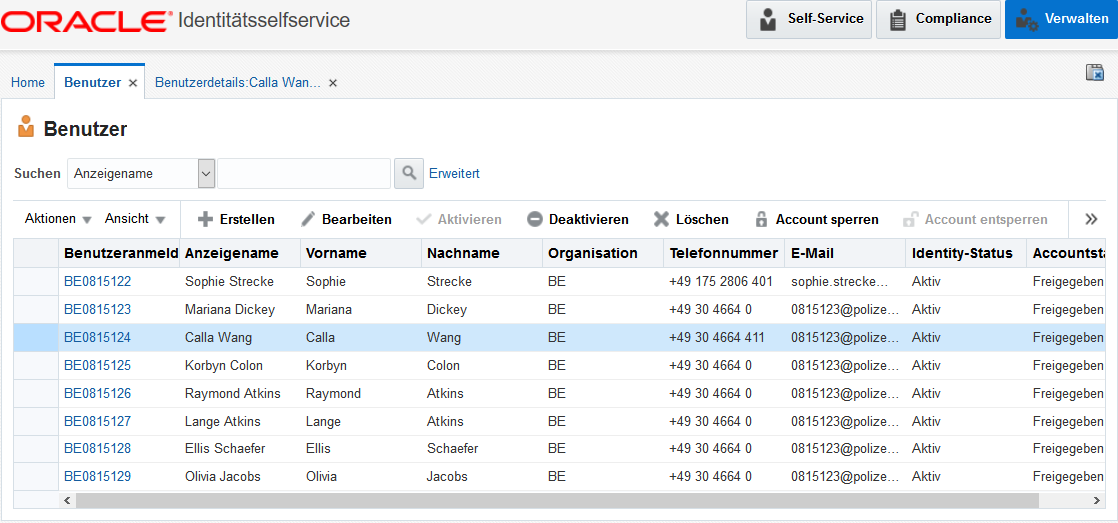
Änderungen einer Identität umfassen folgende Vorgänge

* Kennwort rücksetzen
* Deaktivieren/Aktivieren der Identität
* Sperren/Entsperren der Identität
* Ändern von Attributen

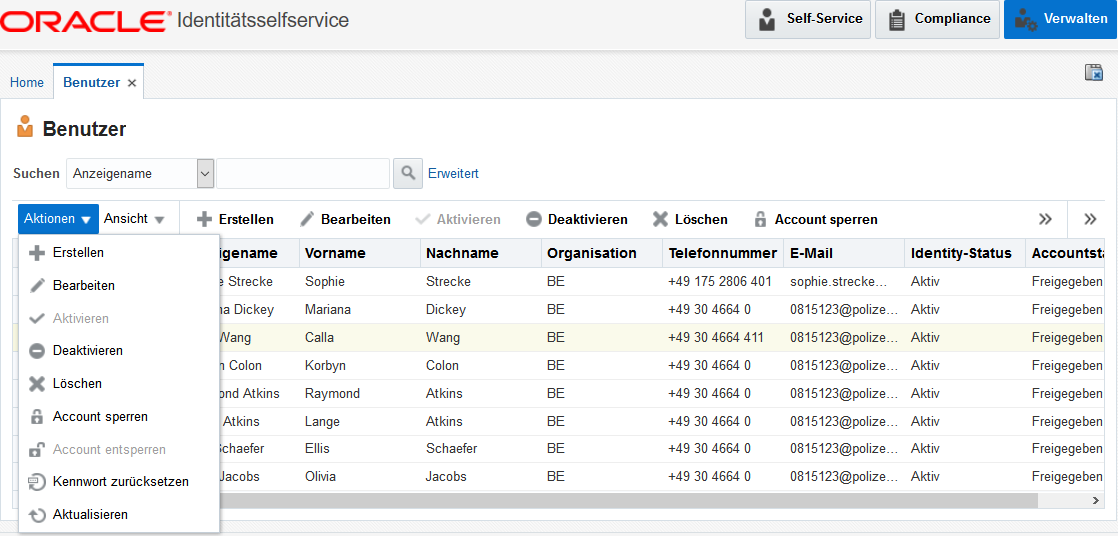
#### Kennwort rücksetzen

Sie können das Kennwort einer Identität zurücksetzen, indem Sie es manuell ändern oder das Kennwort automatisch generieren lassen.

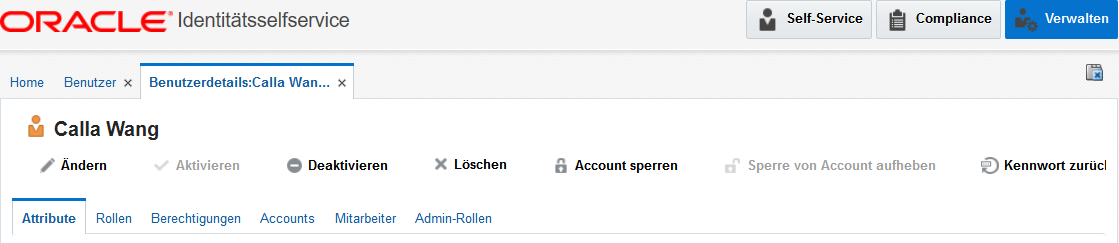
Wählen Sie die Zeile in der sich die Identität befindet, für die Sie das Kennwort zurücksetzen wollen, aus:



Um das Kennwort der Identität zurückzusetzen verfahren Sie folgendermaßen:

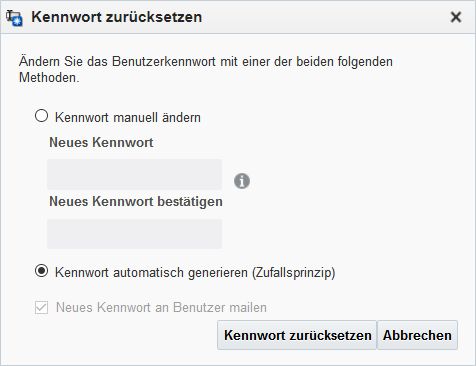


Wählen Sie im Menü **Aktionen** die Option **Kennwort zurücksetzen**. Alternativ können Sie in der Symbolleiste auf **Kennwort zurücksetzen** klicken.



Klicken Sie auf die Benutzeranmeldung der Identität, für die Sie das Kennwort zurücksetzen möchten. Klicken Sie in der Symbolleiste auf **Kennwort zurücksetzen**.

Das Dialogfeld Kennwort zurücksetzen wird angezeigt.



| **Übereinstimmung** | **Verhalten** |
| --- | --- |
| **Kennwort manuell ändern** | Zurücksetzen des Kennworts durch Eingabe eines neuen Kennworts.  Wählen Sie dazu diese Option und geben Sie ein neues Kennwort in die Felder **Neues Kennwort** und **Neues Kennwort bestätigen** ein. Sie können auf das Informationssymbol klicken, um die Kriterien zur Angabe eines Kennworts anzuzeigen.  Wenn Sie die Option **Kennwort manuell ändern** auswählen, können Sie die Option **Neues Kennwort an Benutzer mailen** auswählen, wenn das neue Kennwort per E-Mail an den Benutzer gesendet werden soll. Andernfalls wählen Sie diese Option nicht aus. |
| **Kennwort automatisch generieren** | Kennwort automatisch generieren (zufällig generiert)  Identity Manager wird ermächtigt ein zufälliges Kennwort zu generieren.  Wenn Sie diese Option auswählen, wird standardmäßig die Option **Neues Kennwort an Benutzer mailen** ausgewählt. |

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Es wird empfohlen das neue Kennwort generieren zu lassen. |

Klicken Sie auf **Kennwort zurücksetzen**.

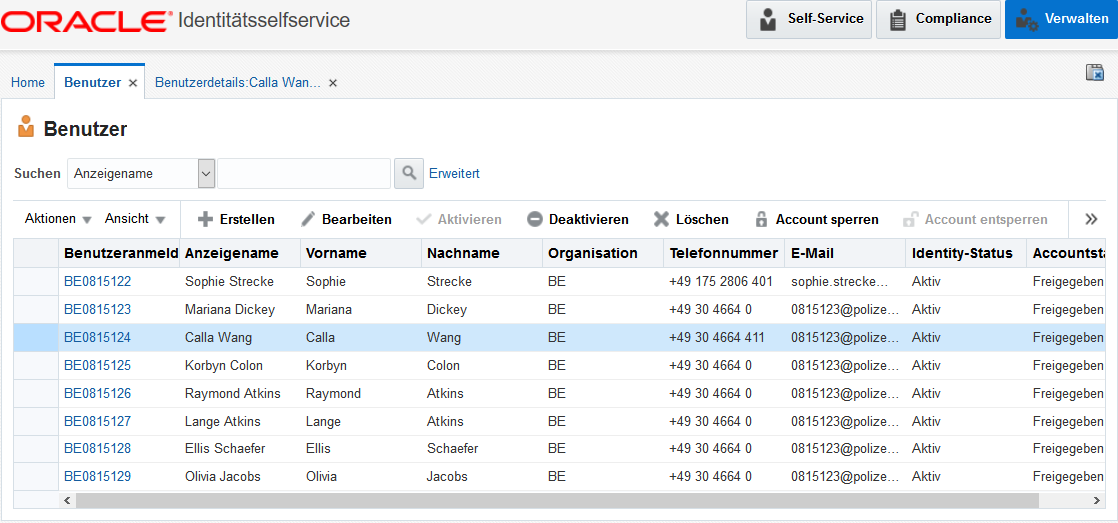
Das Kennwort des geöffneten Benutzers wird zurückgesetzt und falls die Option **Neues Kennwort an Benutzer mailen** ausgewählt wurde diesem per E-Mail zugesandt.

#### Deaktivieren/Aktivieren der Identität

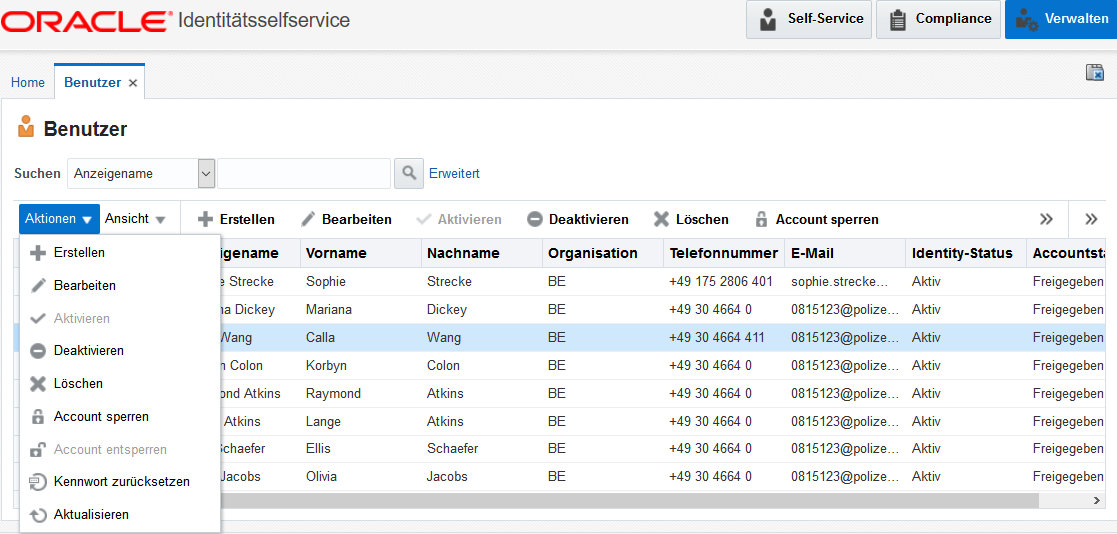
##### Deaktivieren

Sie können eine Identität, die sich im aktivierten Zustand befindet, ab einem bestimmten Datum deaktivieren.

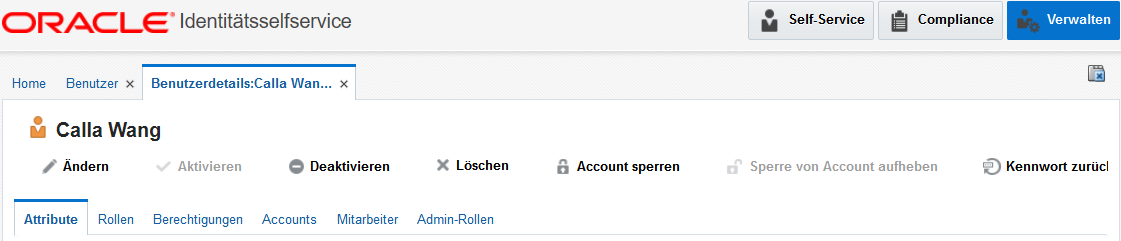
Wählen Sie die Zeile in der sich die zu deaktivierende Identität befindet aus:



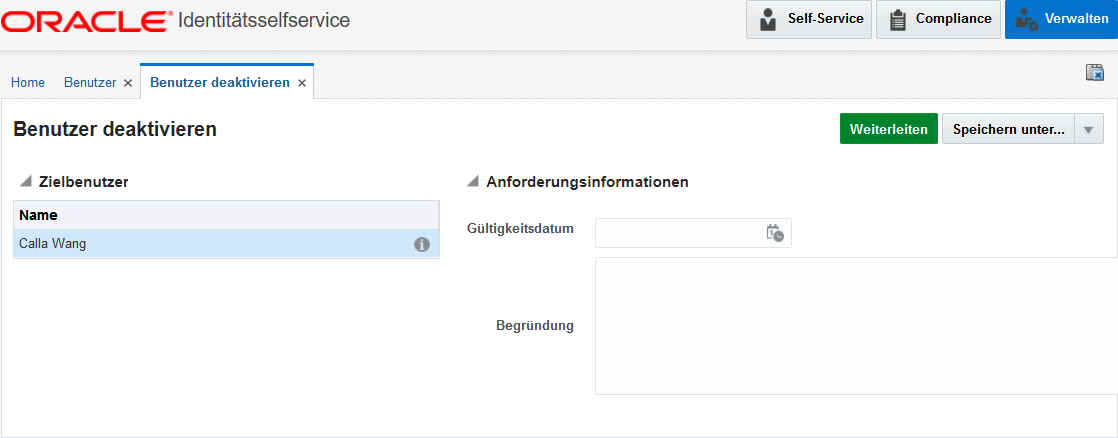
Deaktivieren Sie die Identität auf eine der folgenden Arten:



Wählen Sie im Menü **Aktionen** die Option **Deaktivieren**. Alternativ können Sie in der Symbolleiste auf **Deaktivieren** klicken.



Klicken Sie auf die Benutzeranmeldung der Identität, die Sie deaktivieren möchten. Klicken Sie in der Symbolleiste auf **Deaktivieren**.

Geben Sie in **Benutzer deaktivieren** eine Begründung und ein Datum des Inkrafttretens an, um den ausgewählten Benutzer zu deaktivieren.

Klicken Sie auf **Weiterleiten**.

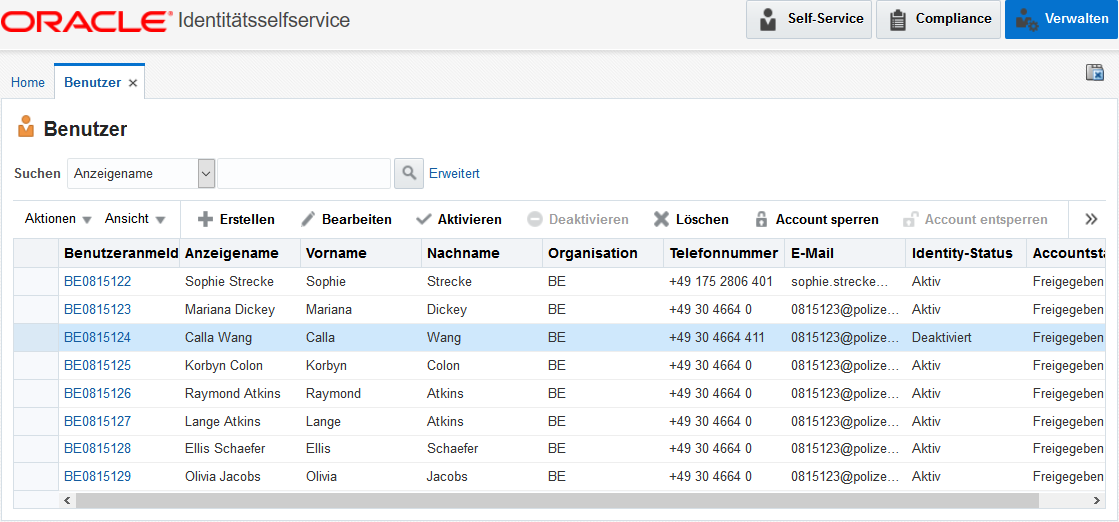


Es wird eine Meldung angezeigt, die besagt, dass die Identität erfolgreich deaktiviert wurde.

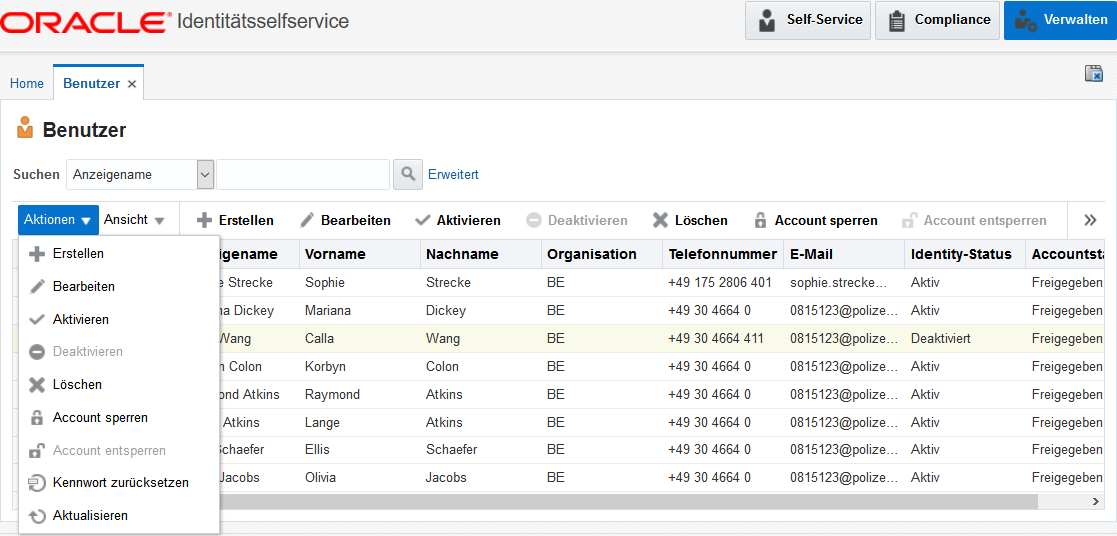
##### Aktivieren

Sie können eine deaktivierte Identität ab einem bestimmten Datum aktivieren.

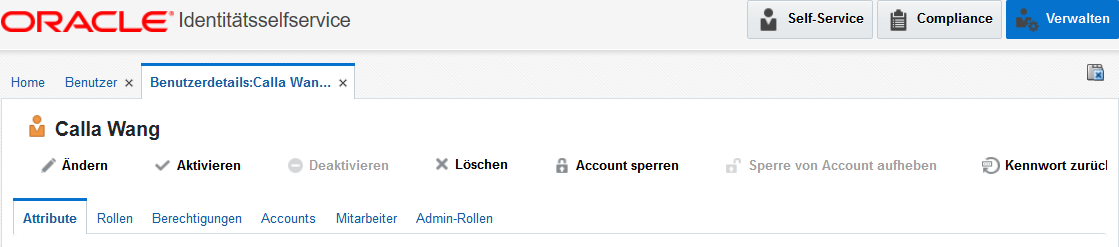
Wählen Sie die Zeile in der sich die zu aktivierende Identität befindet aus:



Deaktivieren Sie die Identität auf eine der folgenden Arten:

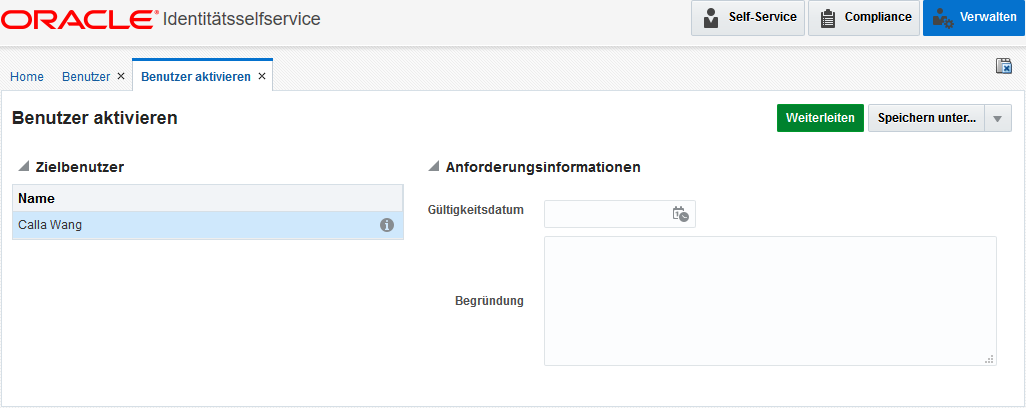


Wählen Sie im Menü **Aktionen** die Option **Aktivieren**. Alternativ können Sie in der Symbolleiste auf **Aktivieren** klicken.



Klicken Sie auf die Benutzeranmeldung der Identität, die Sie deaktivieren möchten. Klicken Sie in der Symbolleiste auf **Aktivieren**.

Geben Sie in **Benutzer aktivieren** eine Begründung und ein Datum des Inkrafttretens an, um den ausgewählten Benutzer zu aktivieren.



Klicken Sie auf **Weiterleiten**.



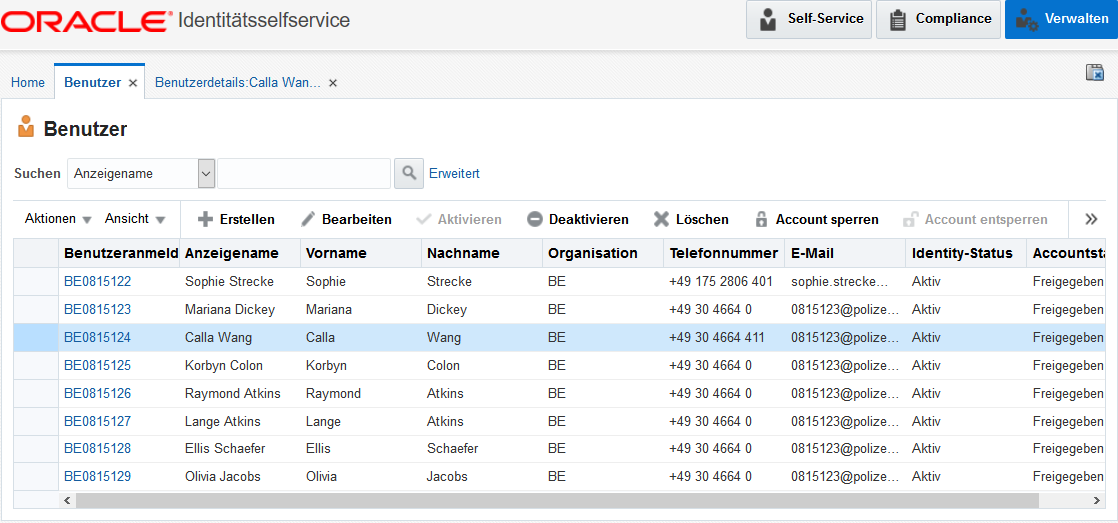
Es wird eine Meldung angezeigt, die besagt, dass die Identität erfolgreich aktiviert wurde.

#### Sperren/Entsperren der Identität

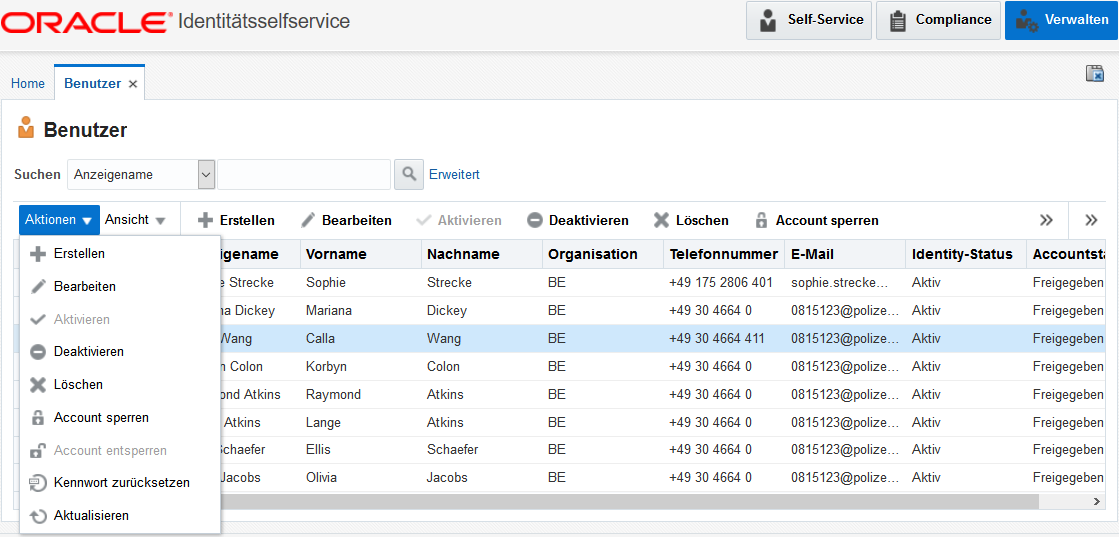
##### Sperren

Sie können das Benutzerkonto das sich im entsperrtem Zustand für Identity Manager für eine Identität sperren.

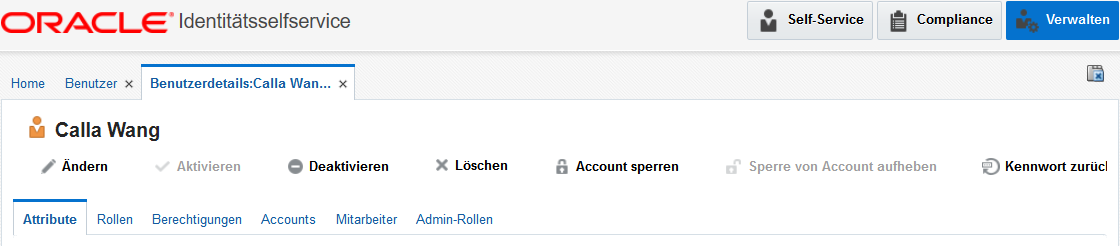
Wählen Sie die Zeile in der sich die zu sperrende Identität befindet aus:



Sperren Sie das Benutzerkonto der Identität auf eine der folgenden Arten:

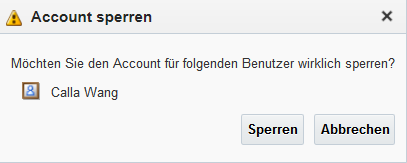


Wählen Sie im Menü **Aktionen** die Option **Account sperren**. Alternativ können Sie in der Symbolleiste auf **Account sperren** klicken.



Klicken Sie auf die Benutzeranmeldung der Identität, die Sie sperren möchten. Klicken Sie in der Symbolleiste auf **Account sperren**.

Bestätigen Sie in dem daraufhin angezeigten Dialogfenster die Sperrung des Benutzerkontos.



Klicken Sie auf **Sperren**.

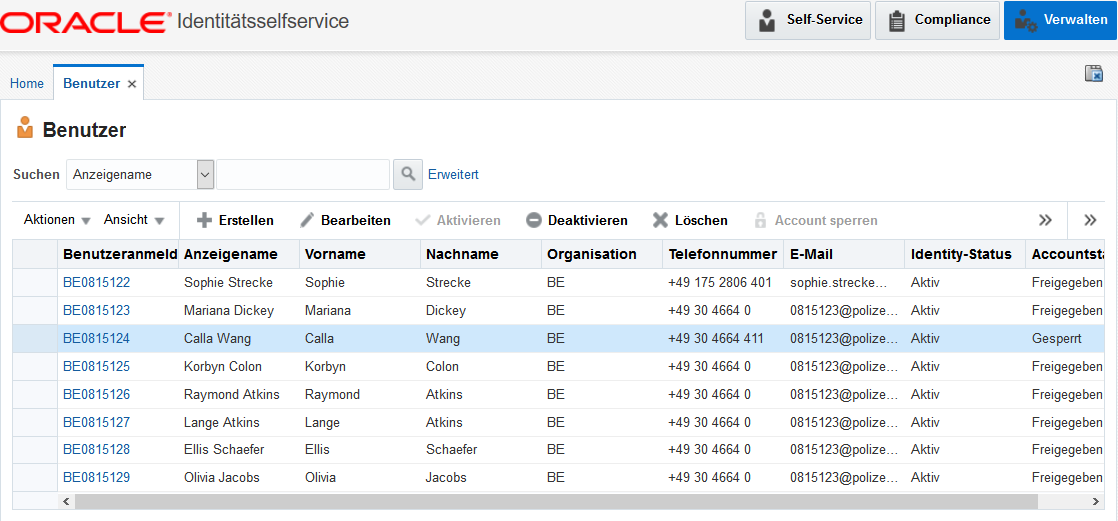


Es wird eine Meldung angezeigt, die besagt, dass die Identität erfolgreich gesperrt wurde.

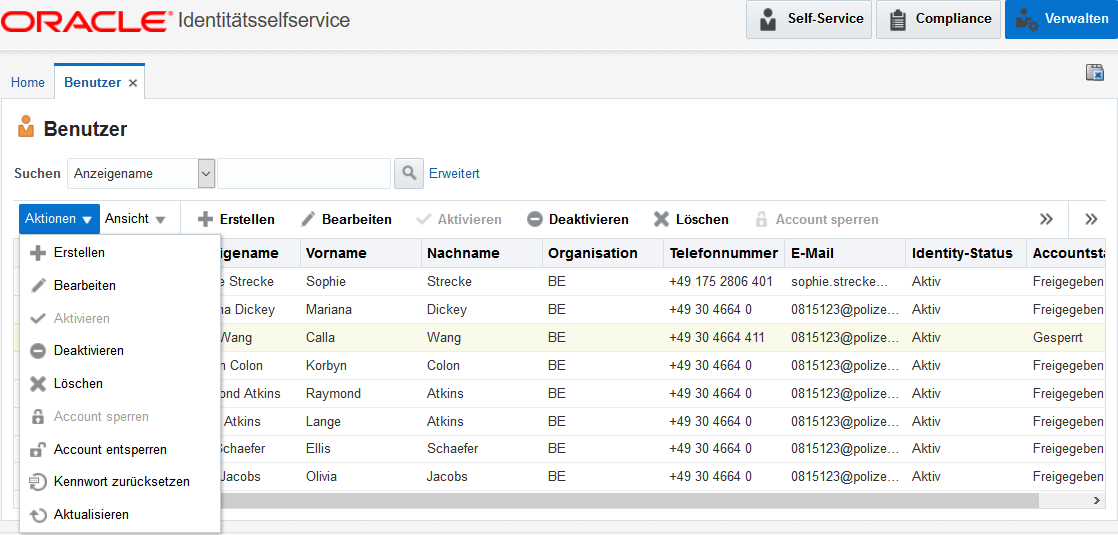
##### Entsperren

Sie können das Benutzerkonto das sich im gesperrtem Zustand für Identity Manager für eine Identität entsperren.

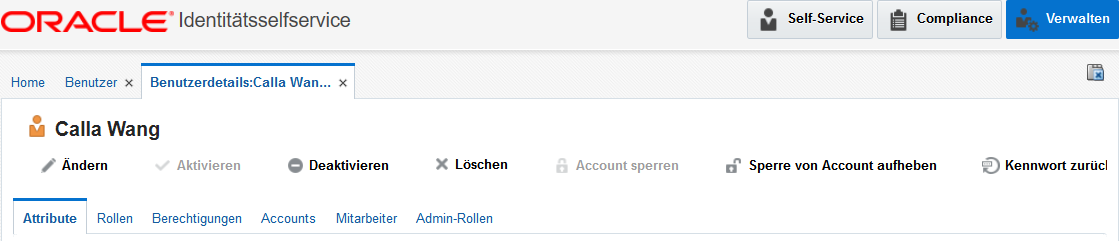
Wählen Sie die Zeile in der sich die zu entsperrende Identität befindet aus:



Sperren Sie das Benutzerkonto der Identität auf eine der folgenden Arten:

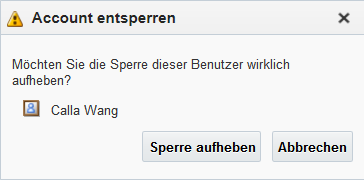


Wählen Sie im Menü **Aktionen** die Option **Account entsperren**. Alternativ können Sie in der Symbolleiste auf **Account entsperren** klicken.



Klicken Sie auf die Benutzeranmeldung der Identität, die Sie entsperren möchten. Klicken Sie in der Symbolleiste auf **Sperre von Account aufheben**.

Bestätigen Sie in dem daraufhin angezeigten Dialogfenster die Entsperrung des Benutzerkontos.



Klicken Sie auf **Sperre aufheben**.



Es wird eine Meldung angezeigt, die besagt, dass die Identität erfolgreich entsperrt wurde.

#### Ändern von Attributen

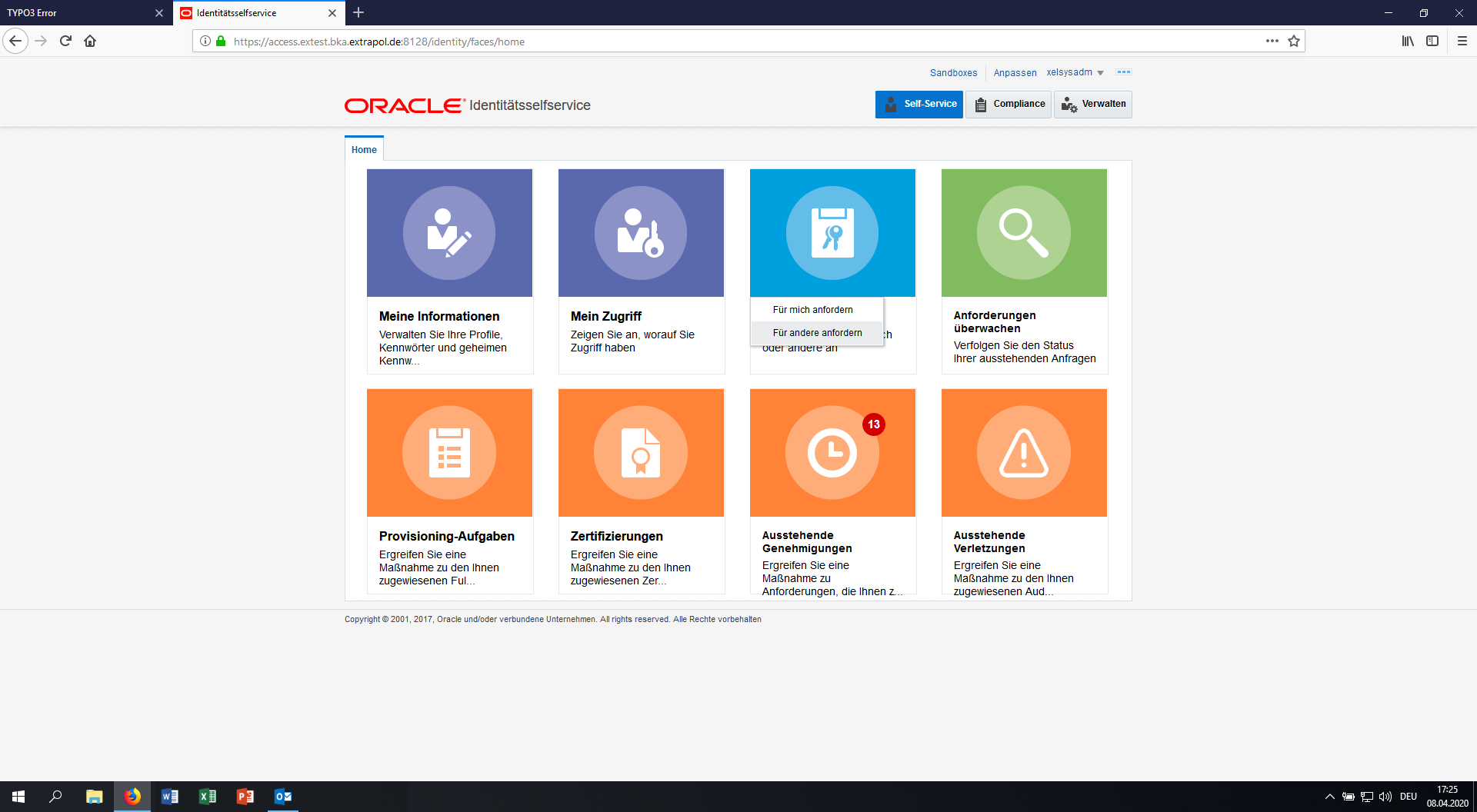
TBD

## Vergabe eFBS Fachanwenderrolle

Nachfolgend wird der manuelle Prozess nach dem Go-Live beschrieben:

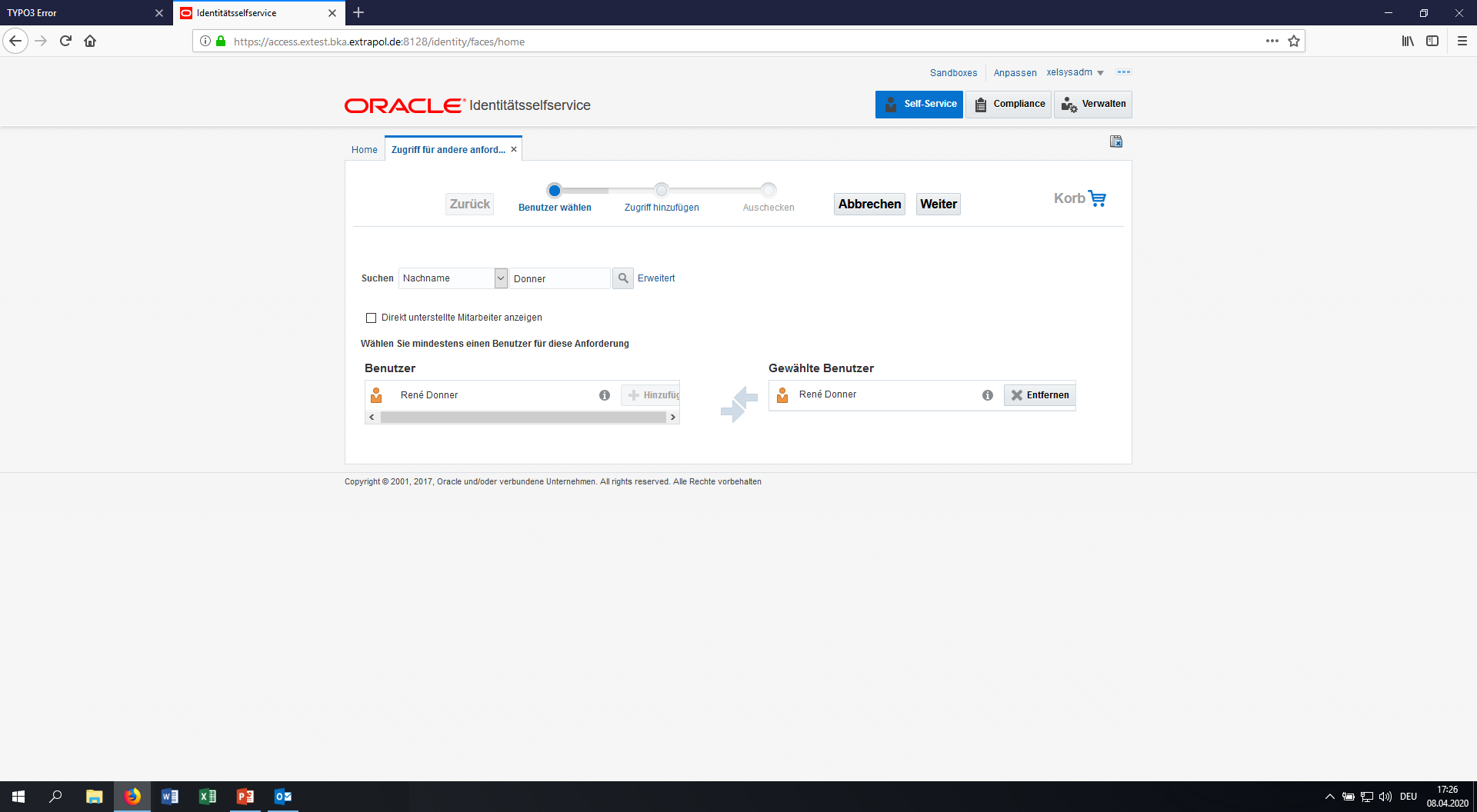
|  | **Achtung** |
| --- | --- |
| Ausschließlich zum Go-Live wird die eFBS Fachanwenderrolle an jede Identität, die klar als Person identifizierbar ist, automatisiert vergeben. |

Wählen Sie im Self-Service Bereich die Kachel **Zugriff anfordern** aus und klicken Sie auf **Für andere anfordern**:



Dadurch wird der Katalog zur Auswahl von Identitäten geöffnet.

#### Auswahl der Identitäten



3

2

1

Nutzen Sie im Suchfeld vorhandene Attribute, um den/die entsprechende\*n Mitarbeiter\*in herauszusuchen. Klicken Sie auf **Hinzufügen** und anschließend auf **Weiter**.

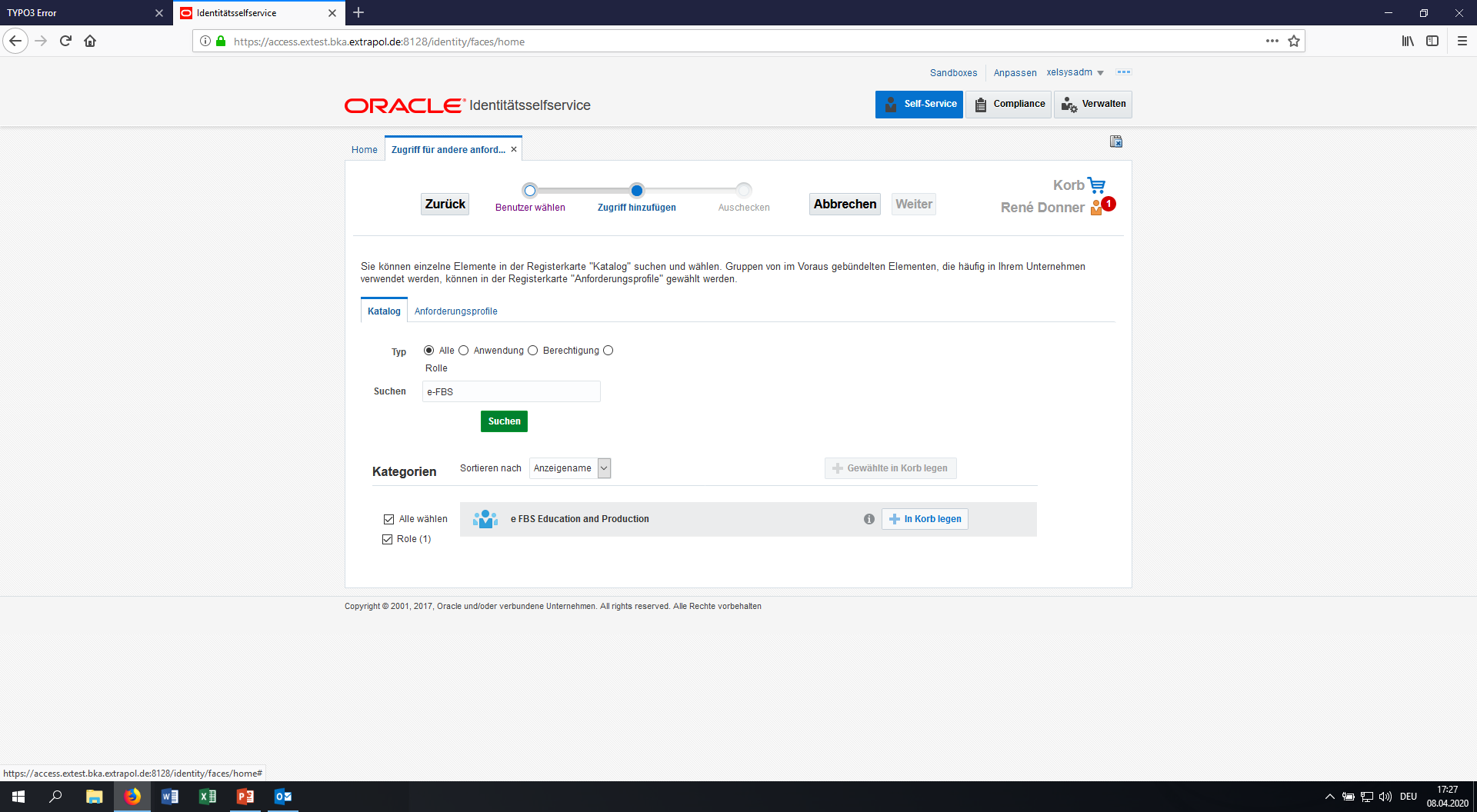
| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Sie können mehr als eine Person gleichzeitig berechtigen. |

Sie gelangen im nächsten Schritt in den Katalog.

#### Auswahl der Rolle

Geben Sie im Suchfeld *eFBS* ein und klicken Sie **Suchen**, es erscheint die *eFBS Fachanwenderrolle*. Mit einem weiteren Klick auf **In Korb legen** wird die Rolle in Ihren Warenkorb gelegt.

|  | **Achtung** |
| --- | --- |
| Der Name der Rolle variiert je Umgebung. Es existieren verschiedene Identity Manager Umgebungen für die verschiedenen eFBS Umgebungen:   * PreProd für eFBS Abnahme und Referenz * Wirk für eFBS Wirk- und Schulungsumgebung |



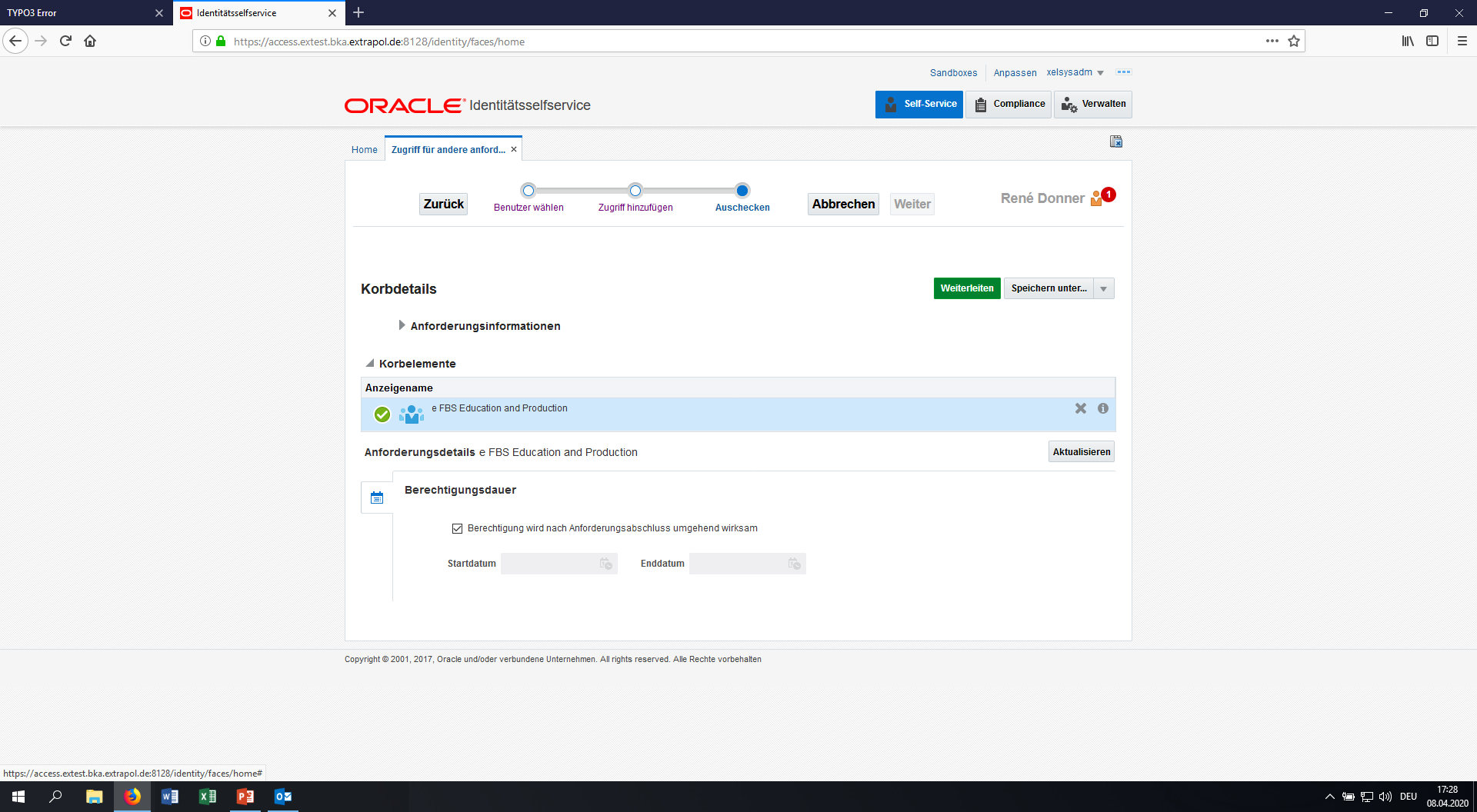
3

2

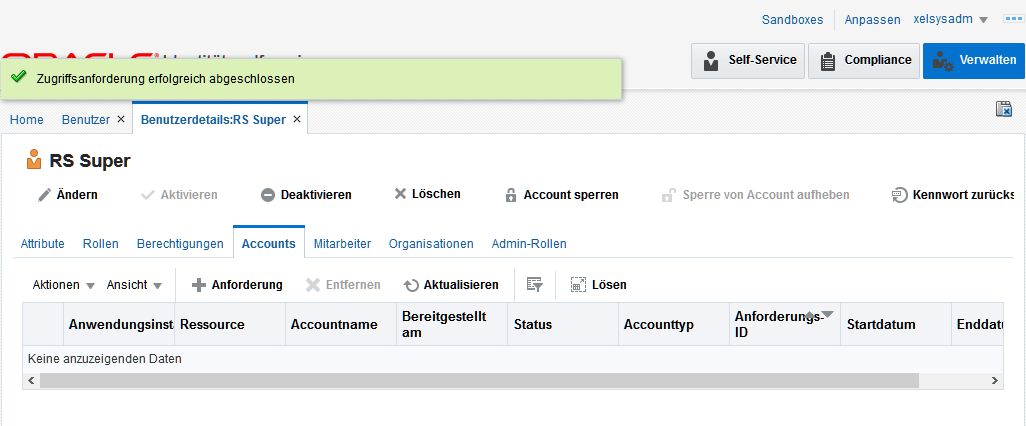
1

#### Anfordern

Sie gelangen zum **Auschecken**, überprüfen Sie hier nochmal ob alle und die richtigen Personen im Warenkorb liegen. Über die Schaltfläche **Weiterleiten** wird die Rolle zur Provisionierung freigegen und der Zugriff binnen weniger Minuten bereitgestellt.



Das System quittiert diese Anforderung mit einer entsprechenden Meldung.



Als Ergebnis der Anforderung des Benutzerkontos solltet dieses in der Liste der zugeordneten **Accounts** angezeigt werden. Gegebenenfalls ist die Anzeige über **Aktualisieren** zu aktualisieren.

## Initiale Anlage von Speziellen eFBS Benutzerkonten

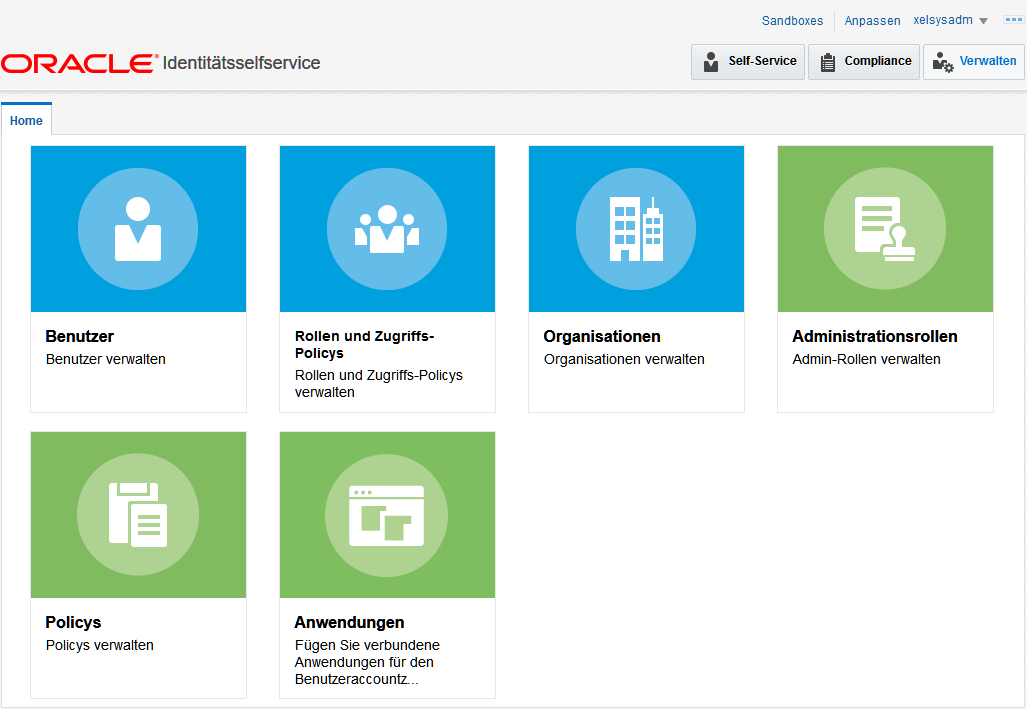
|  | **Achtung** |
| --- | --- |
| Ausschließlich zum Go-Live haben Sie die Möglichkeit eine Liste mit den entsprechenden Mitarbeitern, die einen Account als Globaler Fachadministrator, Globaler Superadministrator, Fachadministrator oder Superadministrator bekommen sollen, an das Projektteam IAM zu übermitteln. Diese wird dann für Sie automatisiert erzeugt. PreProd für eFBS Abnahme und Referenz.  Nachfolgend wird der Regelprozess beschrieben. |

Alle untenstehenden Punkte müssen dabei durchlaufen werden, um einen voll funktionierendes Administrationskonto zu erzeugen:

### Prüfpunkt und Aufruf des Katalogs

Die Bereitstellung der Fach und Superadministratoren erfolgte folgendermaßen:

Wählen Sie globalen den Navigationsbereich **Verwalten** und danach **Benutzer** aus.



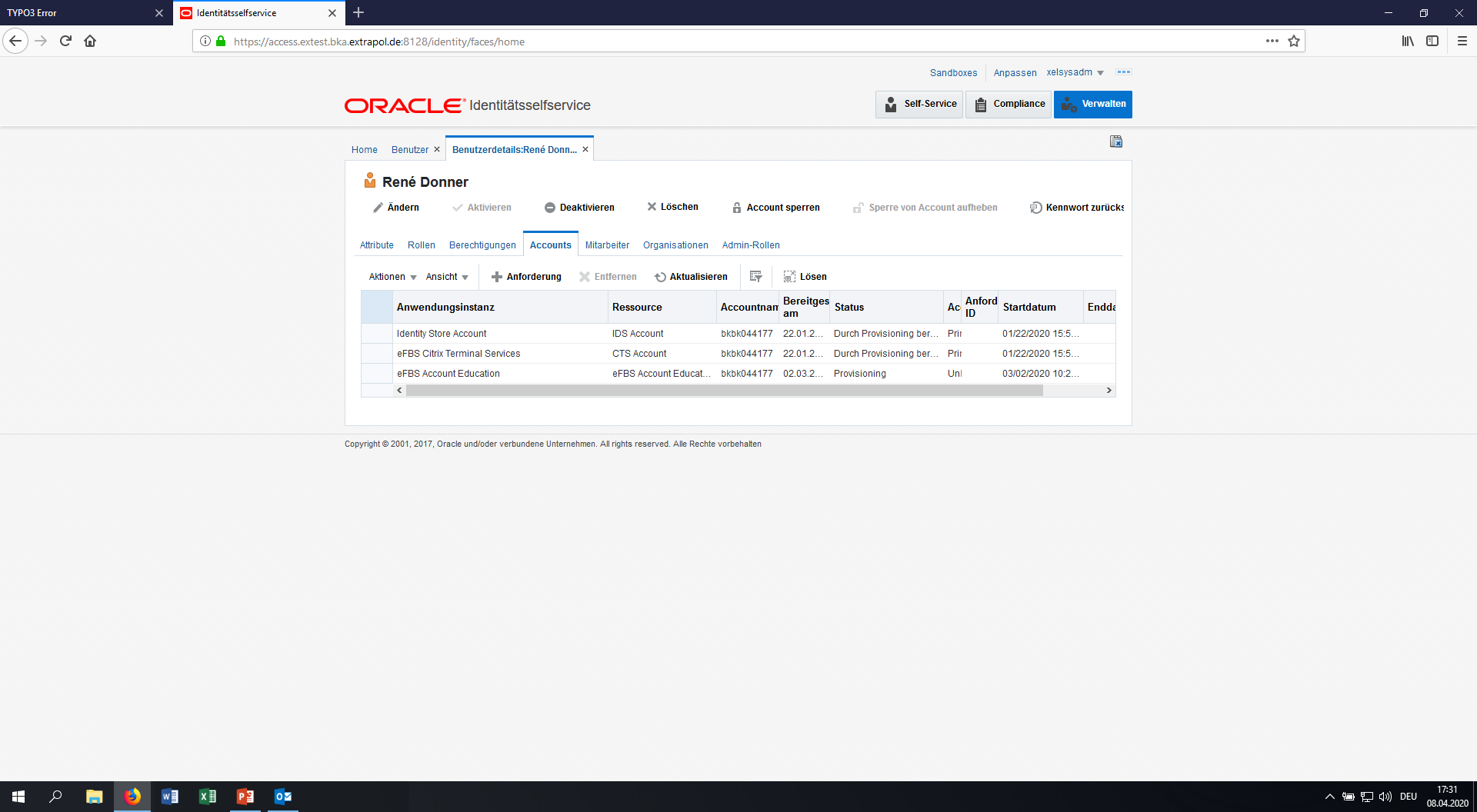
2

1

Nutzen Sie im Suchfeld die Möglichkeiten um den/ die entsprechenden Mitarbeiter\*Inn herauszusuchen. Klicken Sie im Anschluss auf die blau unterlegte Kennung.

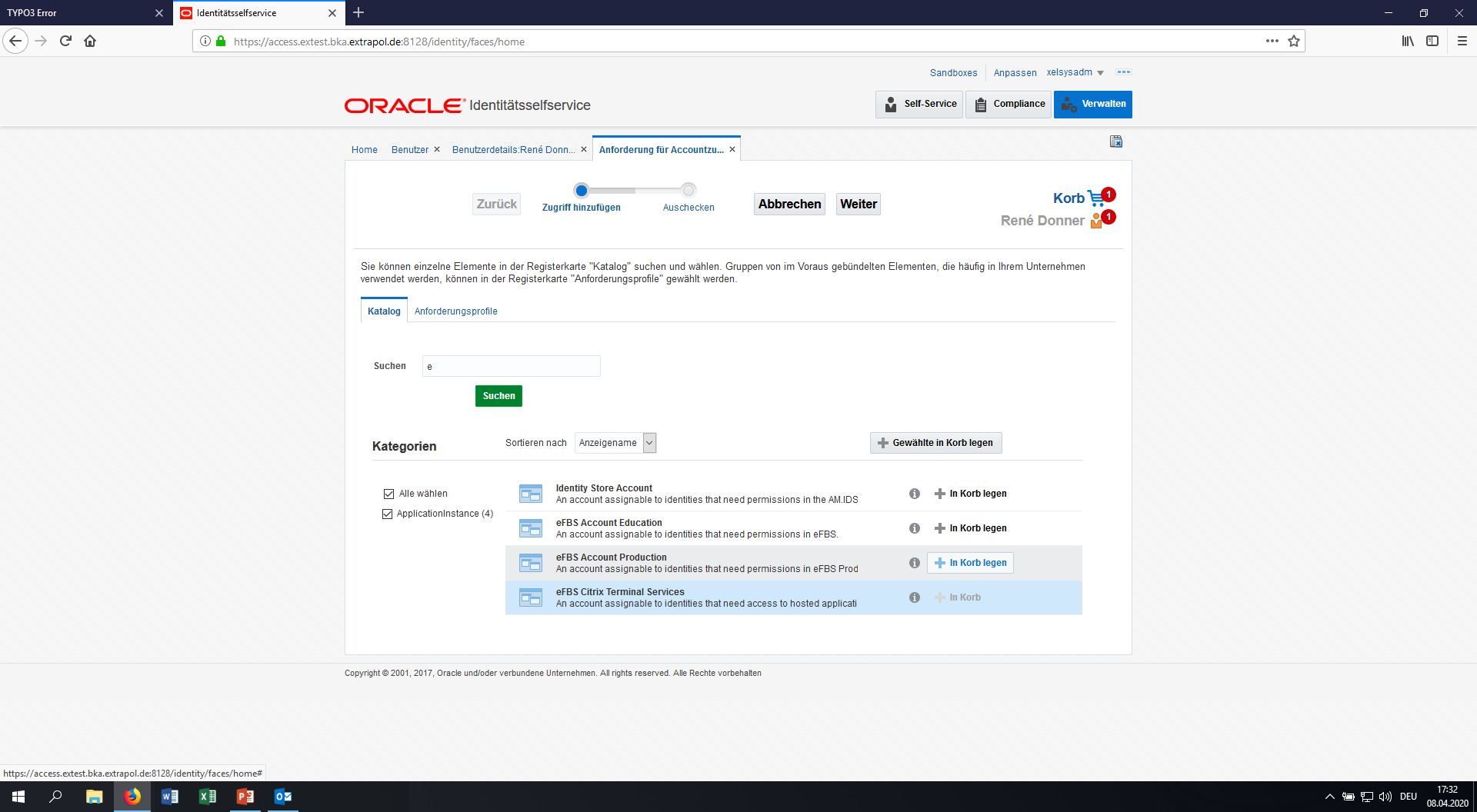
In der Registerkarte **Accounts** erscheinen die der Identität aktuell zugewiesenen Benutzerkonten.

| D:\tt\icon-note-16.png | **Prüfpunkt** |
| --- | --- |
| Vergewissern Sie sich das bereits jeweils ein **eFBS Fachanwender Account** und **CITRIX Terminal Server Account** vorhanden ist. Der **eFBS Fachanwender Account** **MUSS** immer zuerst zugewiesen sein, da aufgrund der unterschiedlichen Namenskonventionen sonst Probleme bei der Anmeldung auftreten können. |



1

Über **Anforderung** wird die Beantragung gestartet und der Katalog geöffnet. Durch Eingabe von *efbs* als Suchkriterium wird die Katalogsuche auf die relevanten Bestandteile eingeschränkt und über **Suchen** zur Ausführung gebracht.



3

2

1

| D:\tt\icon-note-16.png | **Hinweis** |
| --- | --- |
| Ein eFBS Fachadministrator benötigt Benutzerkonten in *eFBS Application Account* **UND** *eFBS Citrix Terminal Services*. |

### Aktualisieren der Warenkorbelemente

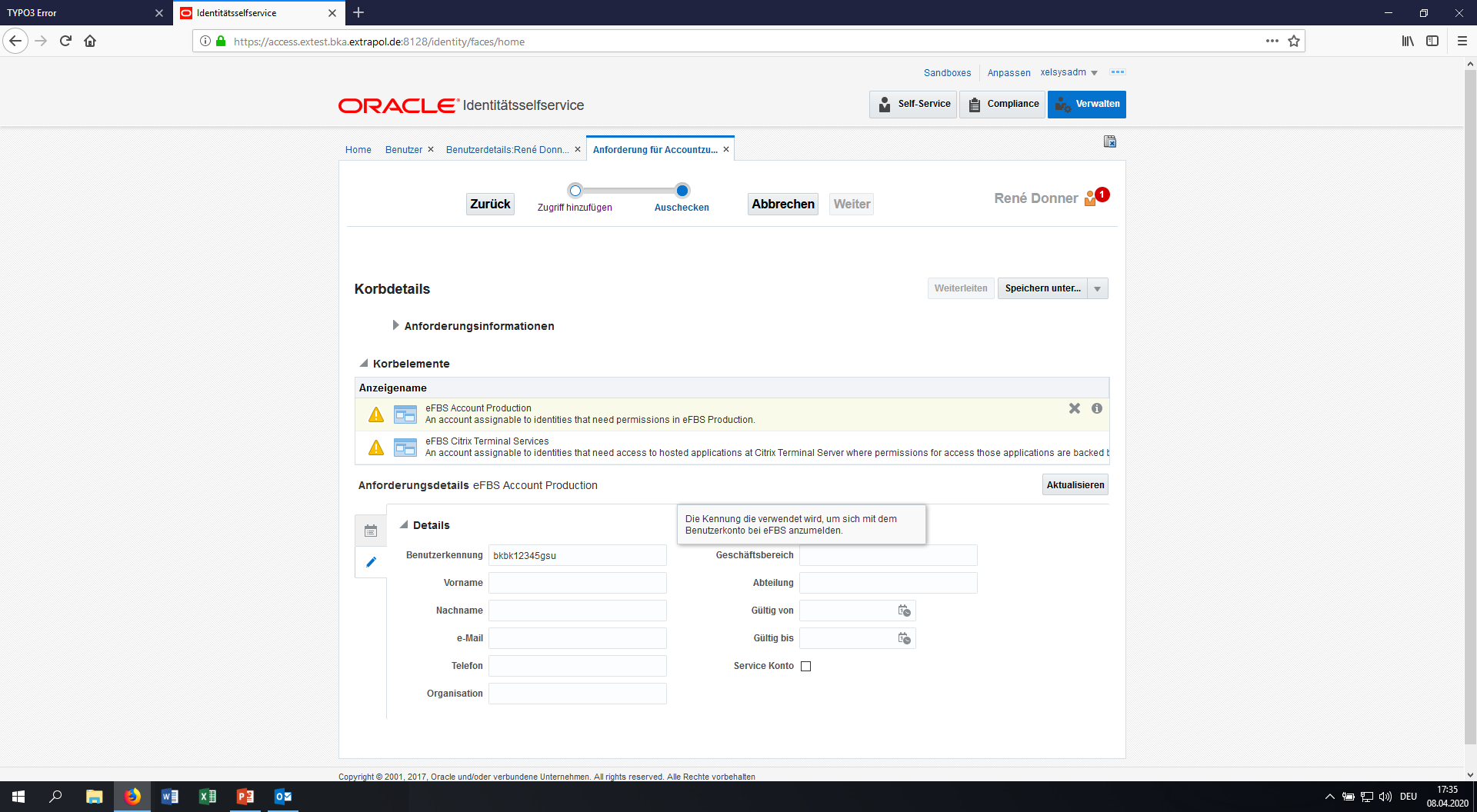
Durch Auswahl des entsprechenden Katalogelements für das anzufordernde Benutzerkonto und *In Korb legen* ist das entsprechende Katalogelement für die Anforderung vorbereitet. Über **Weiter** wird der eigentliche Anforderungsprozess gestartet.

Die Benutzerkonten für einen Fachadministrator, Superadministrator, Globale Fachadministrator und Globale Superadministrator (kurz fa, su, gfa, gsu) **müssen** eine bestimmte Namenskonvention erfüllen. Dies gilt sowohl für den eFBS Account, als auch für den CITRIX Terminalserver Account. Nachfolgend wird beschrieben, wie diese Werte gesetzt werden müssen:

#### eFBS Application Account für fa, su, gfa, gsu

|  | Attribut | Wert | Bedeutung |
| --- | --- | --- | --- |
| Globaler Fachadministrator  [TN-Kürzel]+[Kennung]+ [gfa] | *Benutzerkennung für Globale Fachadministratoren* | Kennung der Identität mit *gfa* als Suffix.  **Beispiel**: bp4711123gfa | Der Anmeldename der *Globale Fachadministratoren* in der Applikation Fachverfahren eFBS |
| Globaler Superadministrator  [TN-Kürzel]+[Kennung]+ [gsu] | *Benutzerkennung für Globale Superadministratoren* | Kennung der Identität mit *gsu* als Suffix.  **Beispiel**: bp4711123gsu | Der Anmeldename der *Globale Superadministratoren* in der Applikation Fachverfahren eFBS |
| Fachadministrator  [TN-Kürzel]+[Kennung]+ [fa] | *Benutzerkennung für Fachadministratoren* | Kennung der Identität mit *fa* als Suffix.  **Beispiel**: bp4711123fa | Der Anmeldename der *Fachadministratoren* in der Applikation Fachverfahren eFBS |
| Superadministrator  [TN-Kürzel]+[Kennung]+ [su] | *Benutzerkennung für Superadministratoren* | Kennung der Identität mit *su* als Suffix.  **Beispiel**: bp4711123su | Der Anmeldename der *Superadministratoren* in der Applikation Fachverfahren eFBS |

Alle anderen Werte für die angezeigten Attribute werden während der Bereitstellung des Benutzerkontos aus den Profildaten der als Begünstigter zu Grunde liegenden Identität ermittelt.



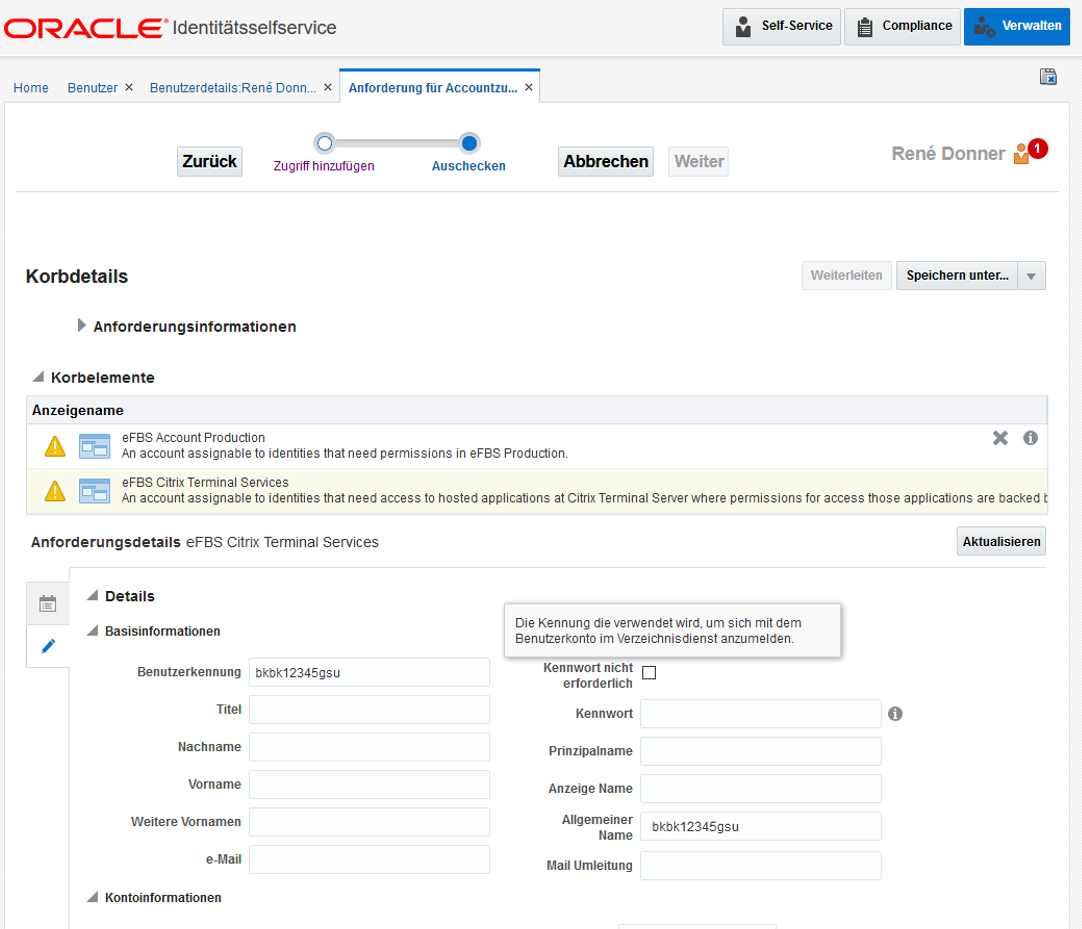
Durch **Aktualisieren** werden die eingegebenen Daten übernommen. Fahren Sie mit dem Citrix Terminal Service Account fort.

#### eFBS Citrix Terminal Services fa, su, gfa, gsu

Sie befinden Sie immer noch im Warenkorb. Zur Aktualisierung des CITRIX Terminalserver Accounts, markieren Sie diesen und beachten die folgende Ausfüllvorschrift:

|  | Attribut | Wert | Bedeutung |
| --- | --- | --- | --- |
| Globaler Fachadministrator  [TN-Kürzel]+[Kennung]+ [gfa] | *Benutzerkennung* | Kennung der Identität mit *gfa* als Suffix.  **Beispiel**: bp4711123**gfa** | Der Benutzername des Globalen Fachadministrators im Microsoft Active Directory der Citrix Terminal Server Farm. |
| *Allgemeiner Name* | Kennung der Identität mit *gfa* als Suffix.  **Beispiel**: bp4711123**gfa** | Der „Common Name“ (beste Übersetzung wäre „Allgemeiner Name“; Microsoft hat das etwas ungünstig als „gemeinsamer Name“ übersetzt) |
| Globaler Superadministrator  [TN-Kürzel]+[Kennung]+ [gsu] | *Benutzerkennung* | Kennung der Identität mit *gsu* als Suffix.  **Beispiel**: bk4711123**gsu** | Der Benutzername des Globalen Superadministrators im Microsoft Active Directory der Citrix Terminal Server Farm |
| *Allgemeiner Name* | Kennung der Identität mit *gsu* als Suffix.  **Beispiel**: bk4711123**gsu** | Der „Common Name“ (beste Übersetzung wäre „Allgemeiner Name“; Microsoft hat das etwas ungünstig als „gemeinsamer Name“ übersetzt) |
| Fachadministrator  [TN-Kürzel]+[Kennung]+ [fa] | *Benutzerkennung* | Kennung der Identität mit *fa* als Suffix.  **Beispiel**: bp4711123**fa** | Der Benutzername des Fachadministrators im Microsoft Active Directory der Citrix Terminal Server Farm. |
| *Allgemeiner Name* | Kennung der Identität mit *fa* als Suffix.  **Beispiel**: bp4711123**fa** | Der „Common Name“ (beste Übersetzung wäre „Allgemeiner Name“; Microsoft hat das etwas ungünstig als „gemeinsamer Name“ übersetzt) |
| Superadministrator  [TN-Kürzel]+[Kennung]+ [su] | *Benutzerkennung* | Kennung der Identität mit *su* als Suffix.  **Beispiel**: bk4711123**su** | Der Benutzername des Superadministrators im Microsoft Active Directory der Citrix Terminal Server Farm. |
| *Allgemeiner Name* | Kennung der Identität mit *su* als Suffix.  **Beispiel**: bk4711123**su** | Der „Common Name“ (beste Übersetzung wäre „Allgemeiner Name“; Microsoft hat das etwas ungünstig als „gemeinsamer Name“ übersetzt). |

Alle anderen Werte für die angezeigten Attribute werden während der Bereitstellung des Benutzerkontos aus den Profildaten der als Begünstigter zu Grunde liegenden Identität ermittelt.

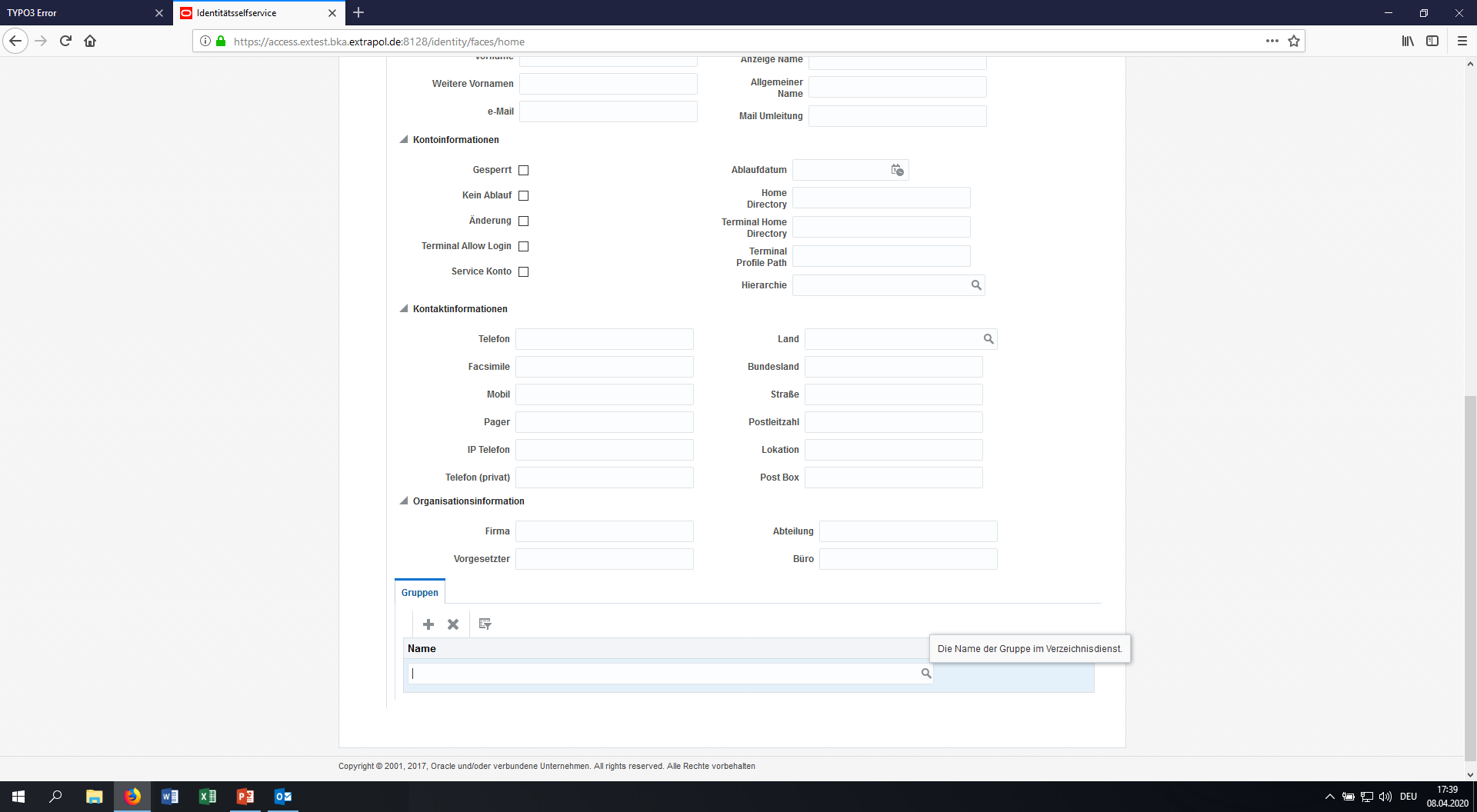


2

1

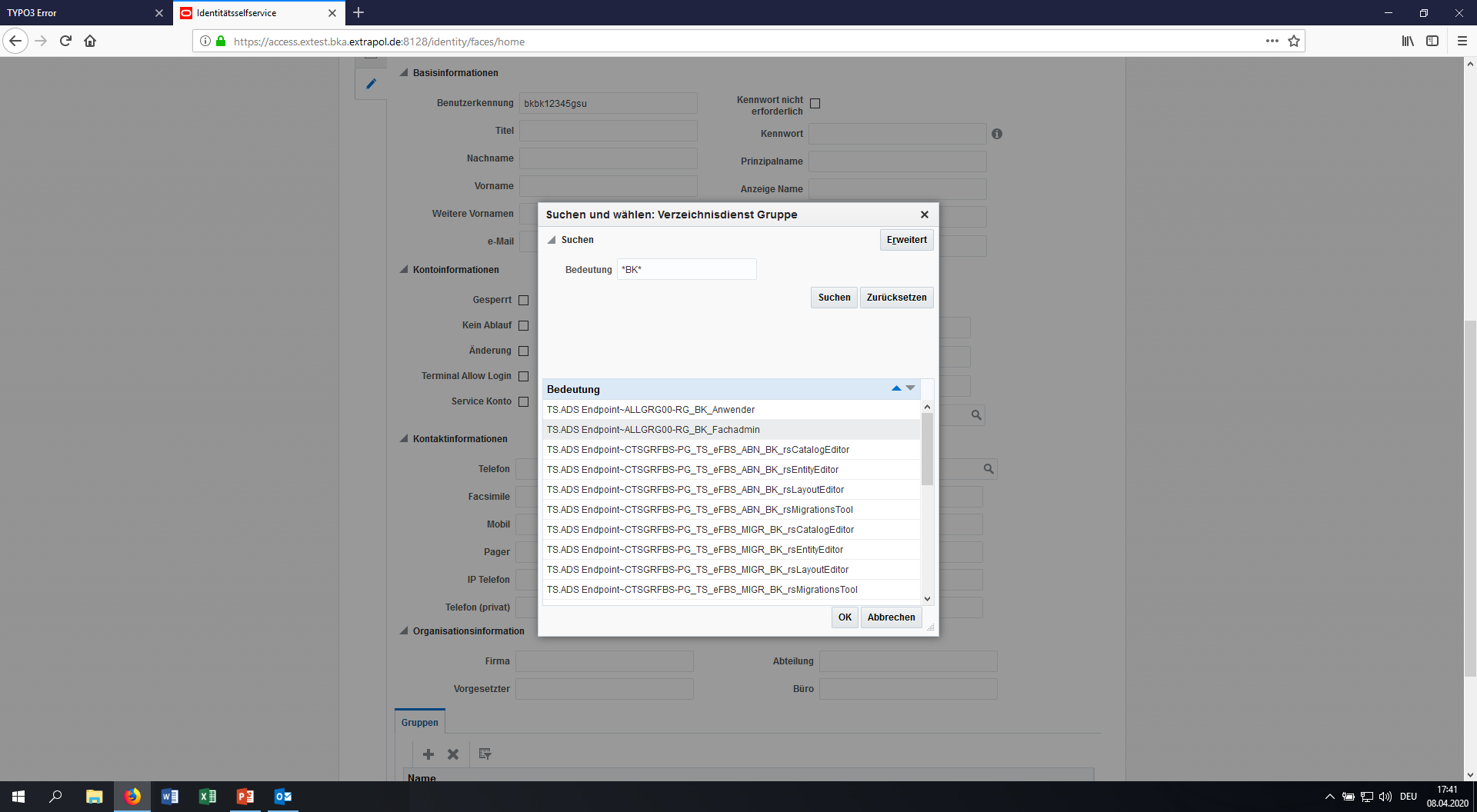
Durch **Aktualisieren** werden die eingegebenen Daten übernommen.

Fügen Sie in einem weiteren Schritt die benötigten CITRIX Anwendungslinks hinzu. Stellen Sie dazu sicher, dass der *eFBS Citrix Terminal Service Account* weiterhin markiert ist, navigieren Sie ganz nach unten und Klicken das **Plus** Symbol:



Über das **Lupe**n Symbol haben Sie die Möglichkeit die entsprechenden Anwendungslink an den Account zu binden. Beachten Sie folgendes:

|  | Admin | Katalogeditor | Entity Editor | Layouteditor | Migrationstool |
| --- | --- | --- | --- | --- | --- |
| Globaler Fachadministrator gfa  [TN-Kürzel]+[Kennung]+ [gfa] | x | x | x | x | x |
| Globaler Superadministrator gsu  [TN-Kürzel]+[Kennung]+ [gsu] | *x* |  |  |  |  |
| Fachadministrator fa  [TN-Kürzel]+[Kennung]+ [fa] | *x* | x | x | x | x |
| Superadministrator su  [TN-Kürzel]+[Kennung]+ [su] | *x* |  |  |  |  |



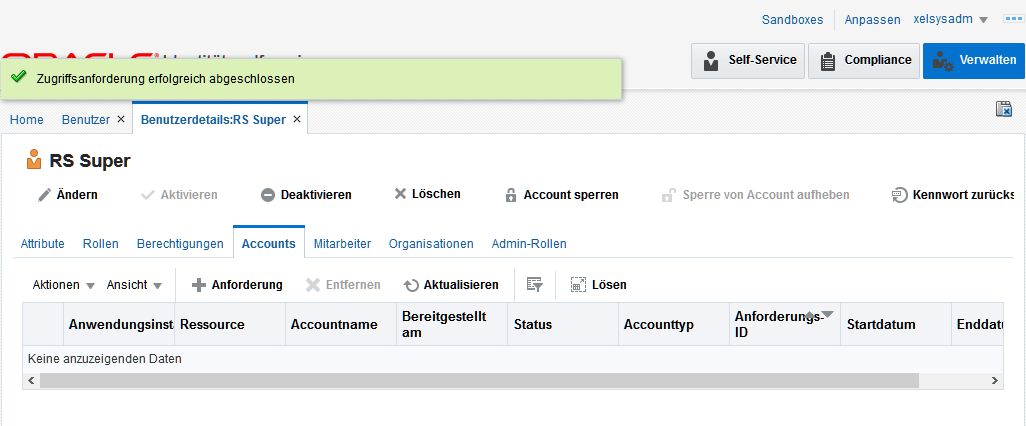
|  | **Achtung** |
| --- | --- |
| Beachten Sie wieder, dass je Umgebung unterschiedliche Links existieren. Die Umgebung erkennen Sie an der Abkürzung:  ABN – Abnahme  MIGR – Migration  Schul – Schulung  Wirk - Wirkumgebung |

Durch Auswahl der entsprechenden Berechtigung und *OK* wird der CITRIX Anwendungs-link ebenfalls in den Warenkorb gelegt.

### Weiterleitung und Abschluss

Durch **Weiterleiten** für die Provisionierung freigegeben.

Das System quittiert diese Anforderung mit einer entsprechenden Meldung.



Als Ergebnis der Anforderung des Benutzerkontos solltet dieses in der Liste der zugeordneten **Accounts** angezeigt werden. Gegebenenfalls ist die Anzeige über **Aktualisieren** zu aktualisieren.

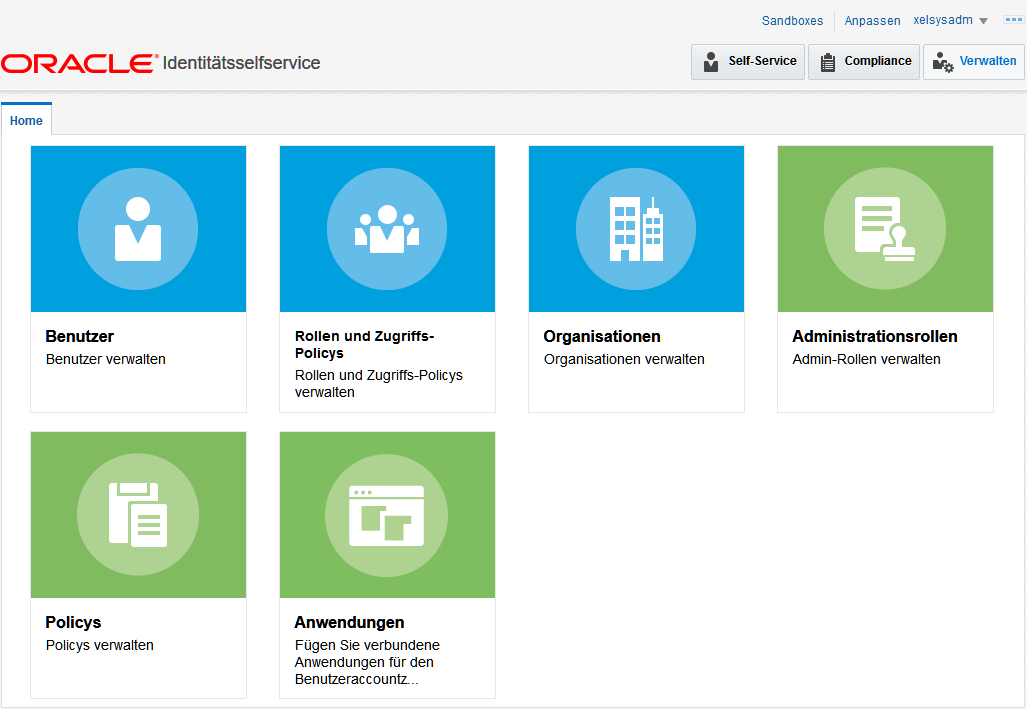
## Kennwortadministration

Kennwortadministratoren werden berechtigt das Kennwort für einen oder mehrere System-konten das Kennwort zusetzen, um sich später mit diesem Kennwort und dem Systemkonto am Fachverfahren anzumelden.

### Setzten des Kennwortes für eFBS Systemaccounts

Vergewissern Sie sich zuvor, ob Sie die entsprechenden Berechtigungen zum Setzten eines Kennworts haben. Im Kapitel eFBS Teilnehmer ist beschrieben welche Berechtigungen Sie dafür benötigen.

Wählen Sie globalen den Navigationsbereich **Verwalten** und danach **Benutzer** aus.

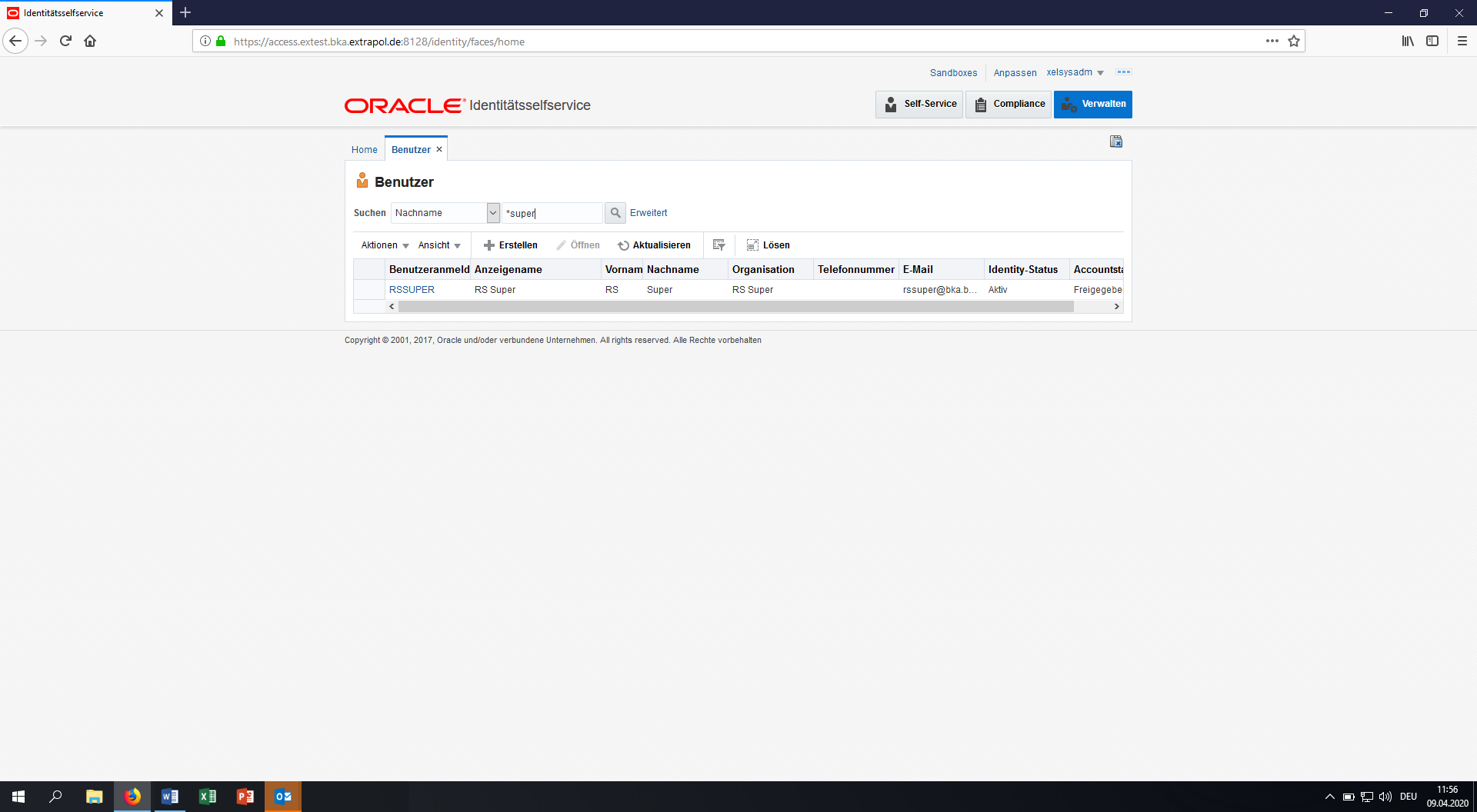


2

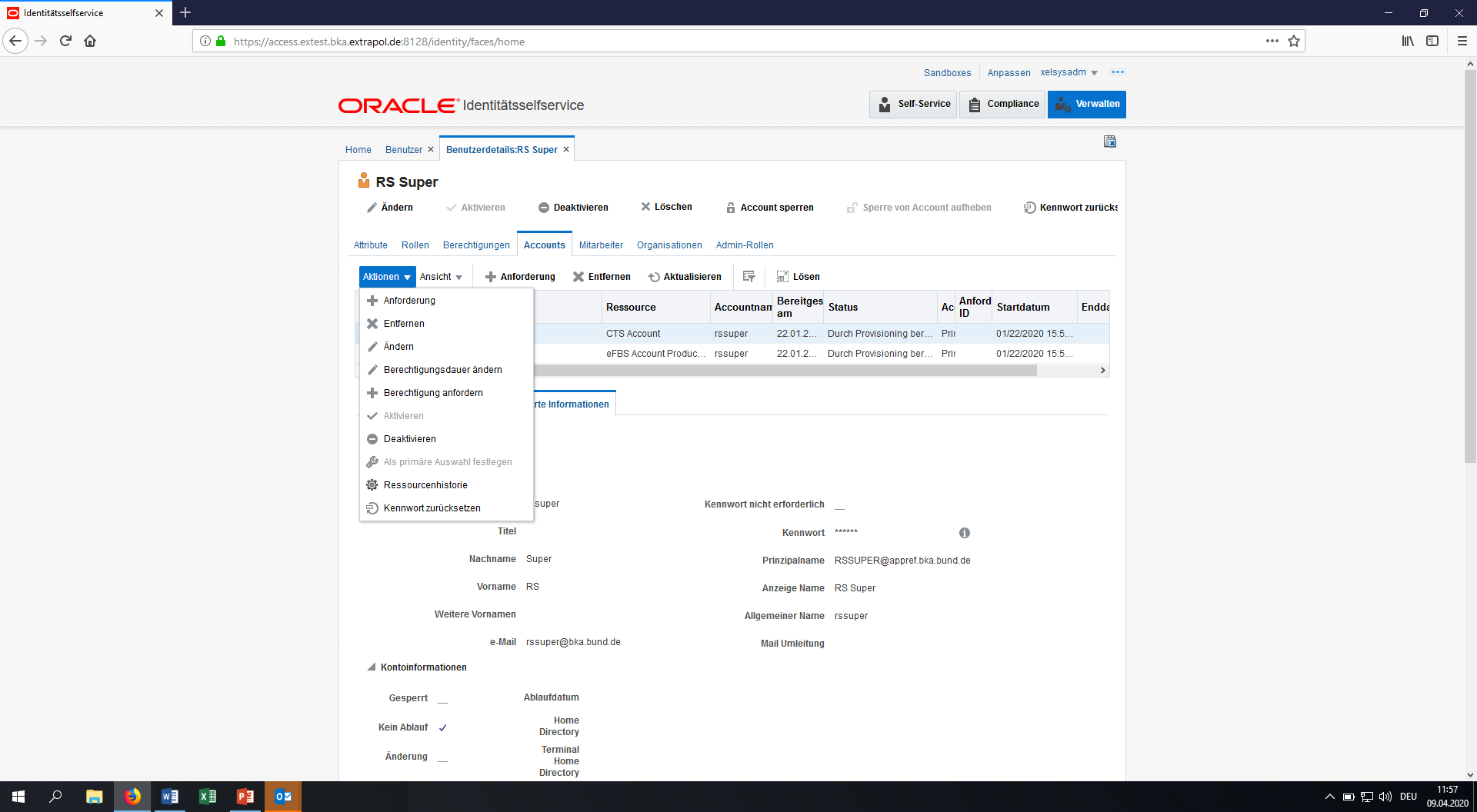
1

Suchen Sie den entsprechenden Account, dessen Passwort Sie setzten möchten.

|  | **Achtung** |
| --- | --- |
| Der Account ist **nur** sichtbar, wenn Sie die Berechtigung zum Setzten des Kennworts haben. |



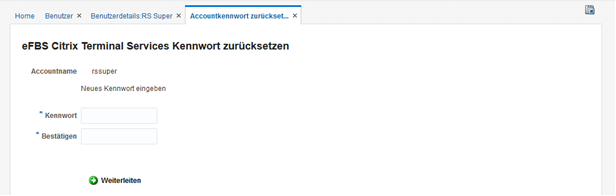
Klicken Sie auf den blau markierten Namen. Sie werden in die Übersicht der vorhandenen **Accounts** geleitet. Damit in unserem Beispiel der rssuper verwendet werden kann, muss das CITRIX Account Passwort gesetzt werden (NICHT das des eFBS Accounts).



1

2

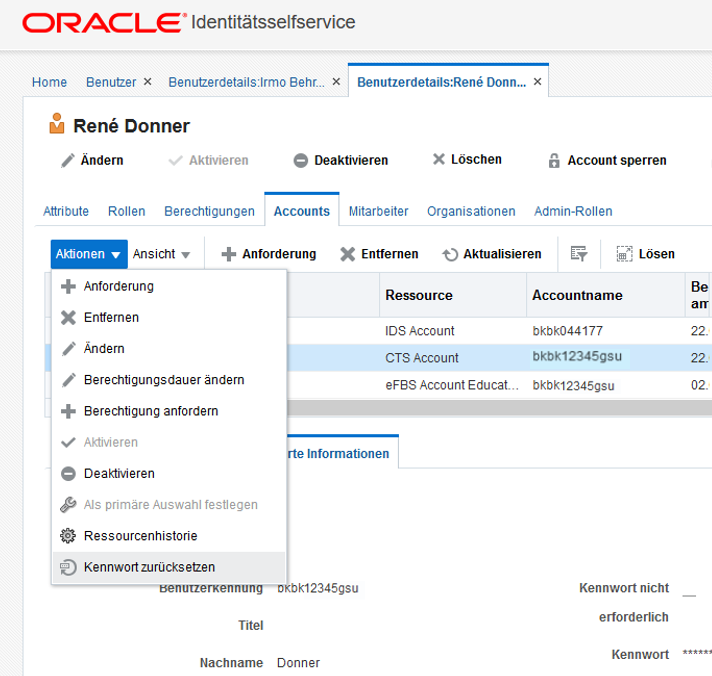
Markieren Sie dazu den CITRIX Account und klicken auf das Drop Down Menü **Aktionen**, hier finden Sie ganz unten den Punkt **Kennwort zurücksetzten**. Sie gelangen hier in die Maske zum Zurücksetzten des Kennwortes. Beim Klick auf die Schaltfläche **Weiterleiten** wird das eingegebene Kennwort übernommen.



### Setzten des Kennwortes für Administrationskonten

Nachdem Sie in Kapitel Initiale Anlage von Speziellen eFBS Benutzerkonteneinen oder mehrere Administrationskonten vom Typ Globaler Fachadministrator, Globaler Superadministrator, Fachadministrator oder Superadministrator angelegt haben, **Müssen** Sie ein Kennwort vergeben, da diese Konten **nicht** mittels Single Sign On authentisiert werden.

Navigieren Sie hier analog zu Kapitel Setzten des Kennwortes für eFBS Systemaccounts zum entsprechenden Mitarbeiter, den Sie freischalten wollen. Danach markieren Sie den **CITRIX Account** mit der Endung **gfa**, **gsu**, **fa** oder **su**:

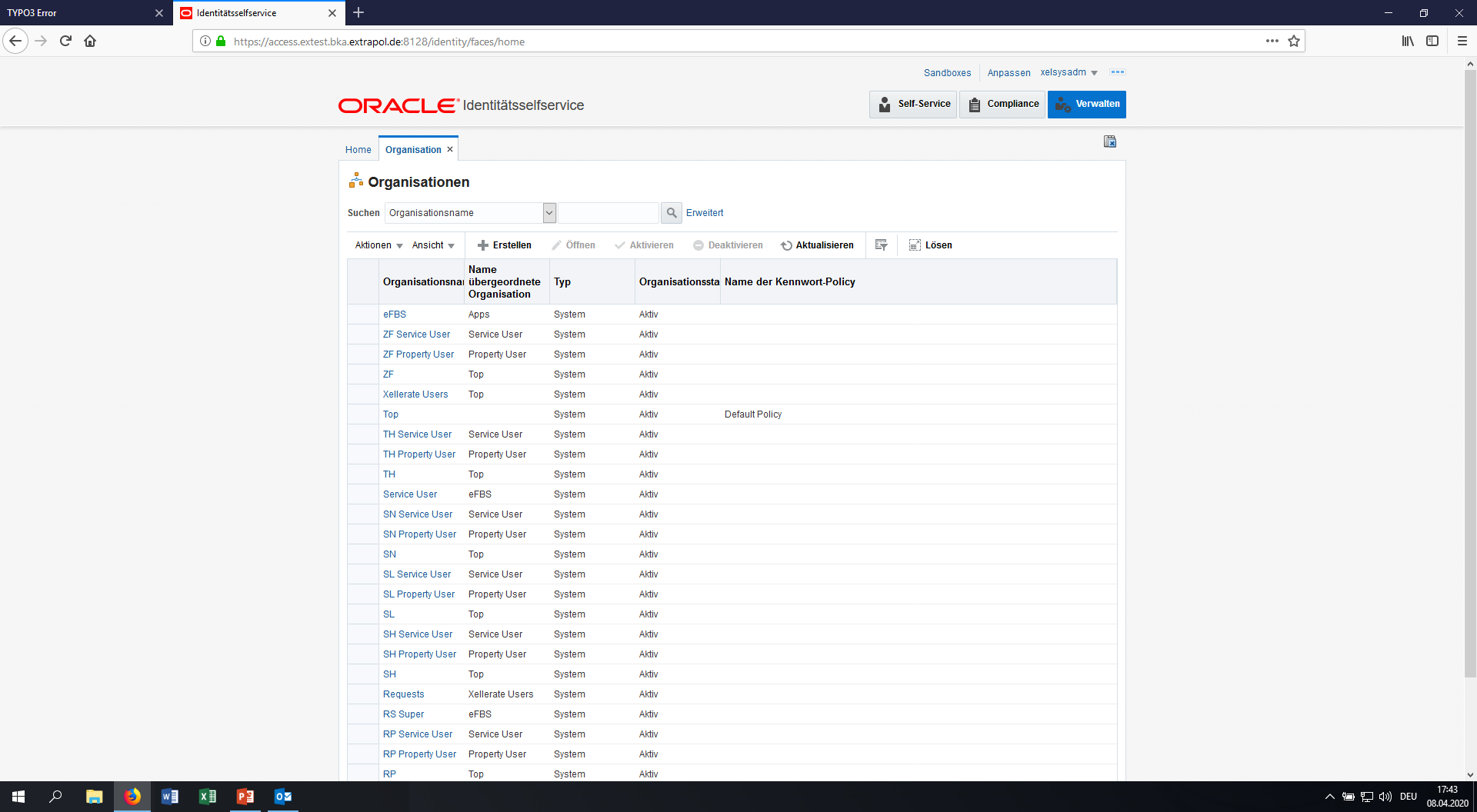


Über das Dropdown Menü **Aktionen** gelangen Sie zum Punkt **Kennwort zurücksetzten**. Beim Klick auf **Kennwort zurücksetzten** werden Sie in die Maske zum Zurücksetzten des Kennwortes weitergeleitet. Beim Klick auf die Schaltfläche **Weiterleiten** wird das eingegebene Kennwort übernommen.

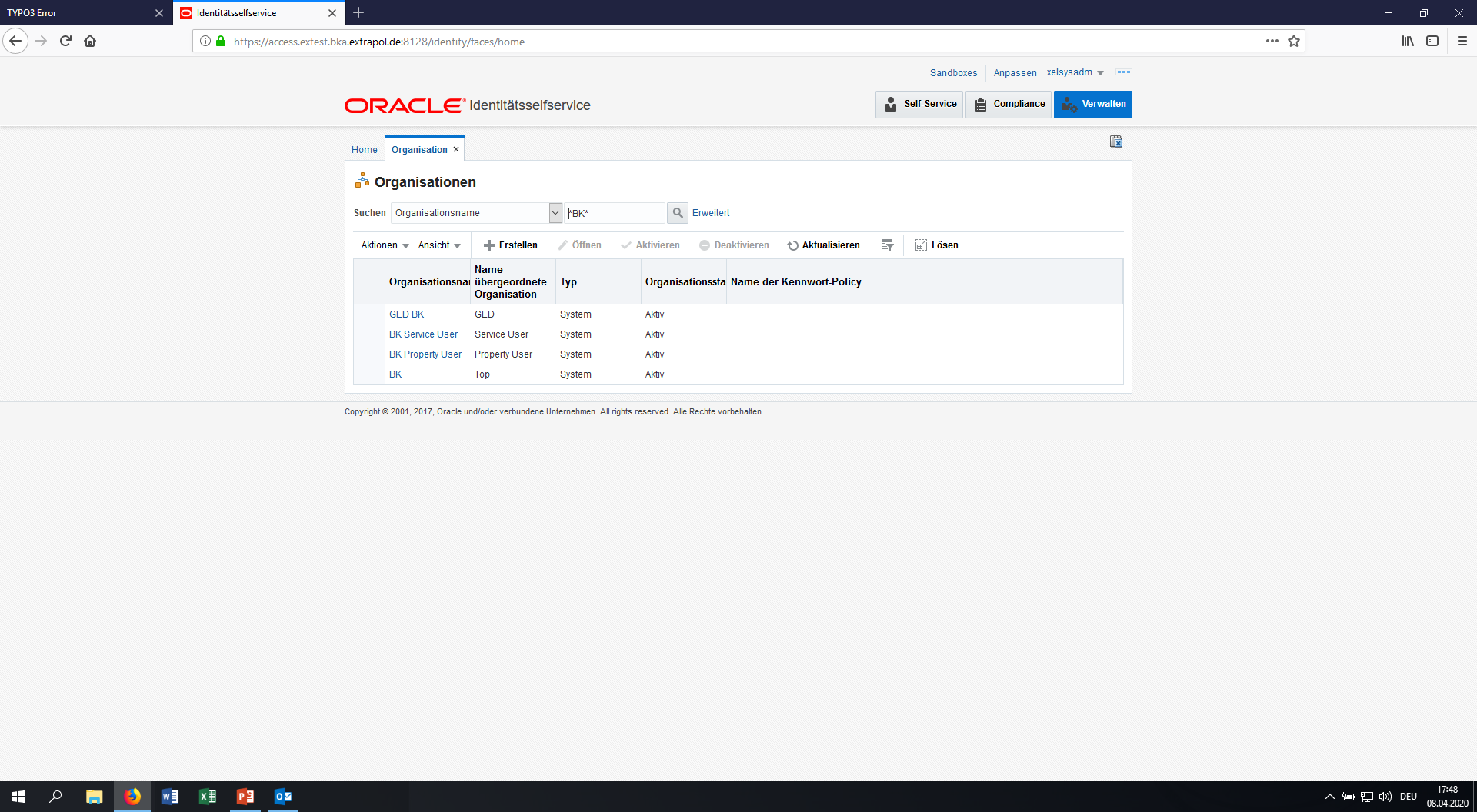
## Ausnahmesituation: Verwendung der „Gemeinsamen Ermittlerdatei (GED)“

Für den GED Fall stehen spezielle User auf Abruf bereit, deren Passwort *nur* noch zur Verwendung freigeschaltet werden muss. Um einen Überblick über die entsprechenden Identitäten zu gewinnen, gehen Sie wie folgt vor:

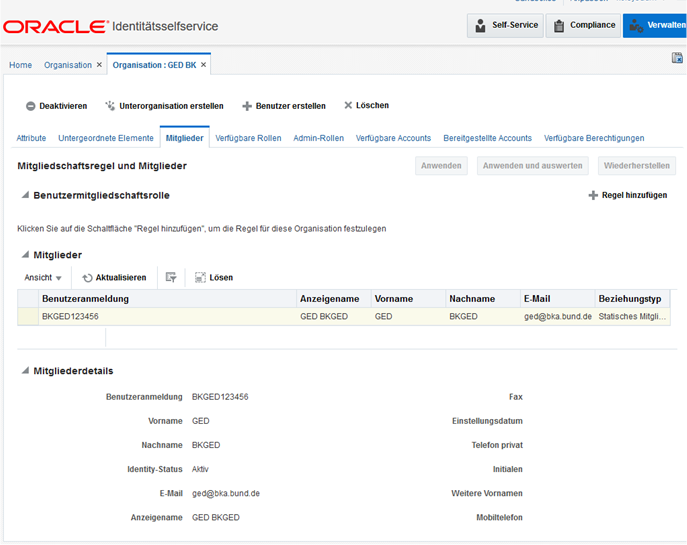
Innerhalb des Verwaltungsbereiches klicken Sie die **Organisation**:



Hier sehen Sie alle Organisationen, die ausschließlich in Ihrer Verwaltungshoheit liegen:



Jeder Teilnehmer egal ob mit oder ohne eigener IAM Infrastruktur verwaltet eine Organisation mit dem Namen „GED“+[TN-Kürzel]“. Hier sind vorgefertigte Zugänge zur GED, deren Kennwort zur Verwendung gesetzt werden muss.



Navigieren Sie nun zurück in den Verwaltungsbereich in die Menükachel **Benutzer** und suchen Sie sich hier den/die GED User aus die Sie freischalten wollen. Verfahren Sie analog zu Kapitel Setzten des Kennwortes für Administrationskonten, um das Kennwort des CITRIX Accounts zu setzten.