Pflichtenheft

Praxis der Softwareentwicklung

Wintersemester 17/18

Authorisierungsmanagement für eine virtuelle Forschungsumgebung für Geodaten

Autoren:

Aleksandar Bachvarov
Anastasia Slobodyanik
Atanas Dimitrov
Khalil Sakly
Houraalsadat Mortazavi Moshkenan
Sonya Voneva

22.11.17

Inhaltsverzeichnis

1 Zielbestimmung

Das Produkt dient zum Authorisierungsmanagement des “V-FOR-WaTer:“Web-Portals. Dadurch können die in dem Web-Portal: registrierte Benutzer: Zugriffsanfragen für Ressourcen senden, Ressourcen nutzen und Ressourcen selbst erstellen. Dabei dient das Produkt auch zur Unterscheidung zwischen Benutzer, Ressourcenbesitzer: und Administrator:.

1.1 Musskriterien

Im Folgenden werden Kriterien aufgelistet, die auf jeden Fall umgesetzt werden.

Benutzer

- Der Benutzer kann Ressourcen lesen, auf die er Zugriffsrechte: hat.
- Der Benutzer kann ein Zugriff-Request dem Ressourcenbesitzer senden, um Zugriffsrechte zu erwerben.
- Der Benutzer bekommt Rückmeldung ob sein Request erfolgreich gesendet war.
- Der Benutzer bekommt eine E-Mail-Benachrichtigung wenn seine Zugriffsanfrage genehmigt/abgelehnt wurde.
- Der Benutzer kann seine eigenen Ressourcen erstellen. Damit wird er den Ressourcenbesitzer dieser Ressourcen.
- Der Benutzer kann seinen Namen im Portal ändern.

Ressourcenbesitzer

- Der Ressourcenbesitzer kann Zugriffsrechte auf seine eigenen Ressourcen auf Request oder freiwillig vergeben.
- Der Ressourcenbesitzer kann freiwillig seine Besitz-Rechte: mit anderen Benutzern teilen.
- Der Ressourcenbesitzer kann ein Loeschen-Request: für seine eigenen Ressourcen dem Administrator senden.
- Der Ressourcenbesitzer kann den Name vom Requst-Absender beim Request sehen.

Administrator

- Der Administrator kann Ressourcen löschen.

- Der Administrator kann Benutzer(vom Portal) entfernen.
- Der Administrator unterstützt die Datenbankverwaltung.
- Der Administrator kann Zugriffsrechte auf Ressourcen beliebig vergeben (ohne selbst Ressourcenbesitzer zu sein).
- Der Administrator kann Besitz-Rechte auf Ressourcen beliebig vergeben (ohne selbst Ressourcenbesitzer zu sein).

1.2 Wunschkriterien

Im Folgenden werden Kriterien aufgelistet, die das Produkt umsetzen kann. Im Verlauf des Entwurfs wird entschieden, welche der Kriterien implementiert werden können.

- Benachrichtigung wenn eine Ressource gelöscht wird (nur an denen Benutzern, die Rechte darauf haben).
- Zugriffsanfrage für mehrere Ressourcen gleichzeitig senden.
- Der Benutzer kann ein Request für Administratorrechte dem Administrator senden.
- Hilfeverweise für den Benutzer.
- Implementierung von Tokens zur Verifizierung von Rechten.
- Mehrmaliges Versagen eines Requests führt zur Benachrichtigung des Administrators.
- Der Ressourcenbesitzer kann Zugriffsrechte auf seine eigenen Ressourcen einer Gruppe von Benutzern vergeben.

1.3 Abgrenzungskriterien

Im Folgenden wird beschrieben, was das Produkt explizit nicht leisten soll.

- Das Produkt dient nicht zur Authentifizierung.
- Das Produkt dient nicht zur Kommunikation zwischen Benutzern.
- Das Produkt unterstützt keine Mobile-Version.
- Die ID:s von Benutzern sind weder sichtbar, noch veränderbar.
- Die E-Mail-Adressen von Benutzern sind nicht veränderbar.
- Das Produkt steht nicht zur Verfügung für Benutzer ohne Account.

2 Produkteinsatz

Das Produkt wird in die Virtuelle Forschungsumgebung (VFU) für die Wasser- und Terrestrische Umweltforschung ("V-FOR-WaTer:") im Rahmen des Netzwerks Wasserforschung Baden-Württemberg eingesetzt. Die VFU legt ihre Schwerpunkte auf die Datenhaltung und den Direkten Zugriff auf Analysewerkzeuge für Daten aus der Wasser- und Umweltforschung. Das Produkt bezieht sich auf die Rechteverwaltung für diese Daten.

2.1 Anwendungsbereiche

- Umweltforschungsbereich
- Datenhaltung

2.2 Zielgruppen

- Administrator(en) der Webseite
- Wissenschaftliche Mitarbeiter von "V-FOR-WaTer:"
- Externe Benutzer des Portals

2.3 Betriebsbedingungen

- Einsatz in einem Webportal mit einer Datenbank:.
- Das Produkt benötigt eine funktionierende Netzverbindung.
- Der Betriebsdauer ist täglich 24 Stunden.

3 Produktumgebung

Das Produkt wird in die virtuelle Forschungsumgebung für Wasser- und Terrestrische Umweltforschung "V-FOR-WaTer:"integriert.
Das Produkt ist weitergehend unabhängig vom Betriebssystem, sofern folgende Produktumgebung vorhanden ist:

3.1 Software

- Server Seite:
  - WebServer Apache

  - SQLite – Datenbank

- Client Seite:
  - Moderne Webbrowser:
    * Chrome
    * Firefox
    * Safari
    * Microsoft Edge

3.2 Hardware

- Server Seite:
  - Netzwerkfähig
  - Rechner, der die Ansprüche der o.g. Server-Software erfüllt.
- Client Seite:
  - Standardrechner
  - Netzwerkverbindung

4 Funktionale Anforderungen

Im Folgenden werden die funktionale Anforderungen: sowohl Musskriterien als auch Wunschkriterien erläutert. Die optionale Funktionalitäten, die sich aus den Wunschkriterien ergeben, sind farblich gekennzeichnet.

4.1 Benutzerfunktionen

/F010/ Profilübersicht:
Der angemeldete Benutzer kann seine personenbezogene Daten (Name, Vorname, E-Mail-Adresse, ID) auf seiner Profilseite sehen.

/F020/ Datenänderung:
Der angemeldete Benutzer kann seinen Namen ändern

/F030/ Ressourcenzugriff:
Der angemeldete Benutzer kann Ressource zugreifen, auf die er Zugriffsrechte hat.
Von Ressourcen, auf die der Benutzer keine Rechte hat, sind nur die glsMeta-Daten sichtbar.

/F040/ Ressourcenerstellung:
Der Benutzer kann neue Ressourcen hochladen, ihre Namen eingeben.

/F050/ Rechte auf Ressourcen anfordern:
Der Benutzer kann Requests an den Ressourcenbesitzer senden, um die Rechte auf gewünschte Ressourcen zu erwerben.

/F060/ Benachrichtigung:
Der Benutzer wird benachrichtigt durch eine E-Mail, wenn sein Request abgelehnt/genehmigt wird.

/F070/ Requestsübersicht:
Der angemeldete Benutzer kann seine abgesendete Requests auf seine Profilseite sehen.

/F080/ Multiple Request:
Der Benutzer kann Zugriffs-Request für mehrere Ressourcen gleichzeitig senden.

/F090/ Administratorrechte anfordern:
Der Benutzer kann ein Request an Administratorrechte senden, um Administratorrechte zu erwerben.

/F100/ Erstellung von Tokens
Der Benutzer bekommt ein Token, mit dem er seine Rechte auf Ressourcen auf einem externen Webserver verifizieren kann.

Beschreibung:

(1) Ein Token wird bei einer Veränderung der Benutzerrechte erstellt bzw. aktualiesiert und dem Benutzer gesendet.

(2) Immer wenn der Benutzer eine externe Webseite besucht, die Ressourcen von V-FOR WaTer verwaltet, wird sein Token für eine leichtere Autorisierung benutzt.

4.2 Administratorfunktionen

/F110/ Bekommen von Löschen-Request
Der Administrator bekommt Request von einem Ressourcenbesitzer zum Löschen von Ressourcen.

Beschreibung:

(1) Nachdem der Ressourcenbesitzer ein Löschen-Request gesendet hat, werden alle Administratoren darüber durch eine Email und durch eine Nachricht im Portal benachrichtigt.

(2) Die Nachricht enthält die Daten des Ressourcenbesitzers und den Namen der Ressource zum Löschen.

(3) Der Administrator kann seine Entscheidung direkt durch eine Interface (zwei Knöpfe “Ja“ oder “Nein“) am Nachrichtbildschirm treffen.

/F120/ Löschen von Ressourcen
Der Administrator darf die Ressourcen im Portal löschen.

Beschreibung:

(1) Die Löschen kann entweder durch die in **/F110/** beschriebene Weise oder auch ohne Request passieren.

(2) Nach der Löschen der Ressource werden alle Ressourcenbesitzer durch eine Email darüber informiert.

/F130/ Rechte gewähren
Der Administrator kann einem Benutzer Zugriff- oder Leserechte einräumen und wieder entziehen.

Beschreibung:

(1) Die Vergabe von Rechte kann entweder durch die in **/F110/** beschriebene Weise oder auch ohne Request passieren.

(2) Nach der Vergabe von Rechte kann der Administrator sie wieder entziehen.

(3) Nach der Entnahme von Rechte kann der Administrator sie wieder vergeben.

/**F140**/ **Benutzer löschen**
Der Administrator kann einen Benutzer löschen.

Beschreibung:

(1) Zusammen mit dem Account werden die personenbezogenen Daten von der Benutzer entfernt.

(2) Der Administrator kann der gelöschten Benutzers Account und Daten nicht wiederherstellen, sondern muss der Benutzer sich nochmal registrieren.

/**F150**/ **Bekommen von Admin-Request**
Der Administrator bekommt Request von einem Benutzer, der vom Administrator verlangt, ein Administrator zu werden.

Beschreibung:

(1) Der Ablauf ist ähnlich zu dem in /**F110**/. Unterschiedlich ist, dass jeder Benutzer dieses Request senden kann und natürlich die Sache(nämmlich die Adminrechte), die durch das Request angefragt wird.

/**F160**/ **Benutzer blockieren**
Der Administrator kann einen Benutzer blockieren, damit dieser sich nicht anmelden kann.

Beschreibung:

(1) Wenn der Benutzer blockiert ist, sind seinem Account und Daten nicht gelöscht, sondern kann er sich nicht mehr anmelden.

(2) Der Administrator kann der blockierende Benutzer wieder zum anmelden zulassen.

/**F170**/ **Benutzer suchen**
Es kann ein Benutzer anhand von Vorname, Nachname durch den Administrator gesucht werden.

Beschreibung:

(1) Nach der Suche wird der gesuchte Benutzer dann angezeigt und er steht zur Verfügung.

4.3 Ressourcenbesitzerfunktionen

/F180/ Übersicht der Requests:
Eine Liste von Requests ist auf Profilseite vorhanden.

Beschreibung:

(1) Nach der Anmeldung wird dem Ressourcenbesitzer eine Liste von Requests, die von anderen Benutzern gesendet sind, angezeigt.

/F190/ Übersicht der Ressourcen:
Es steht eine Liste von Ressourcen auf der Profilseite zur verfügung.

Beschreibung:

(1) Nach der Anmeldung wird dem Ressourcenbesitzer eine Liste von Ressourcen, die von ihm besessen sind, angezeigt.

/F200/ Übergabe der Zugriffsrechte:
Der Besitzer kann Zugriffsrechte ohne Request an anderen Benutzer vergeben.

/F210/ Request auf Zugriffsrechte ablehnen/genehmigen:
Der Ressourcenbesitzer bekommt von anderen Benutzern Zugriff-Request.

Beschreibung:

(1) Der Ressourcenbesitzer kann die gesendeten Requests, die von anderen Benutzern zur Anforderung einer Zugriffsrechte gesendet wurden, entweder ablehnen oder annehmen.

(2) In beiden Fälle(Genehmigung/Ablehnung) werden der entsprechenden Benutzern benachrichtigt.

(3) Im Fall Genehmigung bekommt der Benutzer Die Zugriffsrechte auf gewünschte Ressourcen.

/**F220**/ **Übergabe der Besitz-Rechte:**
Der Ressourcenbesitzer kann freiwillig seine Besitz-Rechte mit anderen Benutzern teilen.

/**F230**/ **Löschen-Request senden:**
Der Ressourcenbesitzer ist in der Lage zum Löschen seinen Ressourcen ein Request dem Administrator zu senden.

/**F240**/ **Löschbenachrichtigungen:**
Beim Löschen einer Ressource werden allen Ressourcenbesitzer benachrihtigt.

/**F250**/ **Zugriffsrechte einer Gruppe vergeben:**
Der Ressourcenbesitzer kann Zugriffsrechte auf seine eigenen Ressourcen einer Gruppe von Benutzern vergeben.

Beschreibung:

(1) Die Vergabe von Zugriffsrechte kann entweder durch die in /**F180**/ und /**F190**/ beschriebene Weise einzeln oder auch kumulativ passieren.

5 Produktdaten

5.1 Benutzerdaten

/**D010**/ Vorname

/**D020**/ Nachname

/**D030**/ ID

/**D040**/ E-Mail Adresse

5.2 Sonstiges

/**D050**/ Ressourcenliste, die der Benutzer besitzt

/**D060**/ Status (Administrator, Benutzer)

5.3 Ressourcendaten

/**D070**/ Titel

/**D080**/ Erstellungsdatum

/**D090**/ Besitzer

/**D100**/ Leser

6 Nichtfunktionale Anforderungen

/**NF010**/ Eine Änderung von Rechten wird nach nächster Seitenaktualisierung sichtbar.

/**NF020**/ Zur Erstellung eines Requests sind maximal 5 Schritte nötig.

/**NF030**/ Zur Erstellung einer neuen Ressource sind maximal 5 Schritte nötig.

/**NF040**/ Eine Änderung von Rechten führt nicht zur Veränderung von Ressourcen.

/**NF050**/ Hilfeverweise

/**NF060**/ Zeitverhalten - angemessen

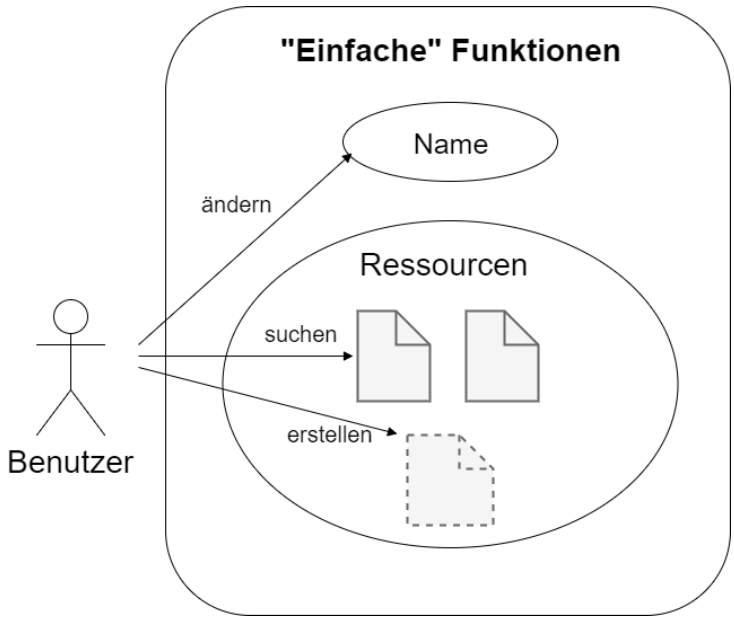
7 Systemmodelle

7.1 Szenarien

Einfache BenutzerFunktionen

Alice hat sich vor kurzem verheiratet und möchte darum ihren Familiennamen im Portal von "V-FOR-WaTer:"ändern. Sie loggt sich im System ein und sieht ihr Profil. Dann klickt sie auf dem Knopf "Name editieren"und tippt ihren neuen Namen ein.

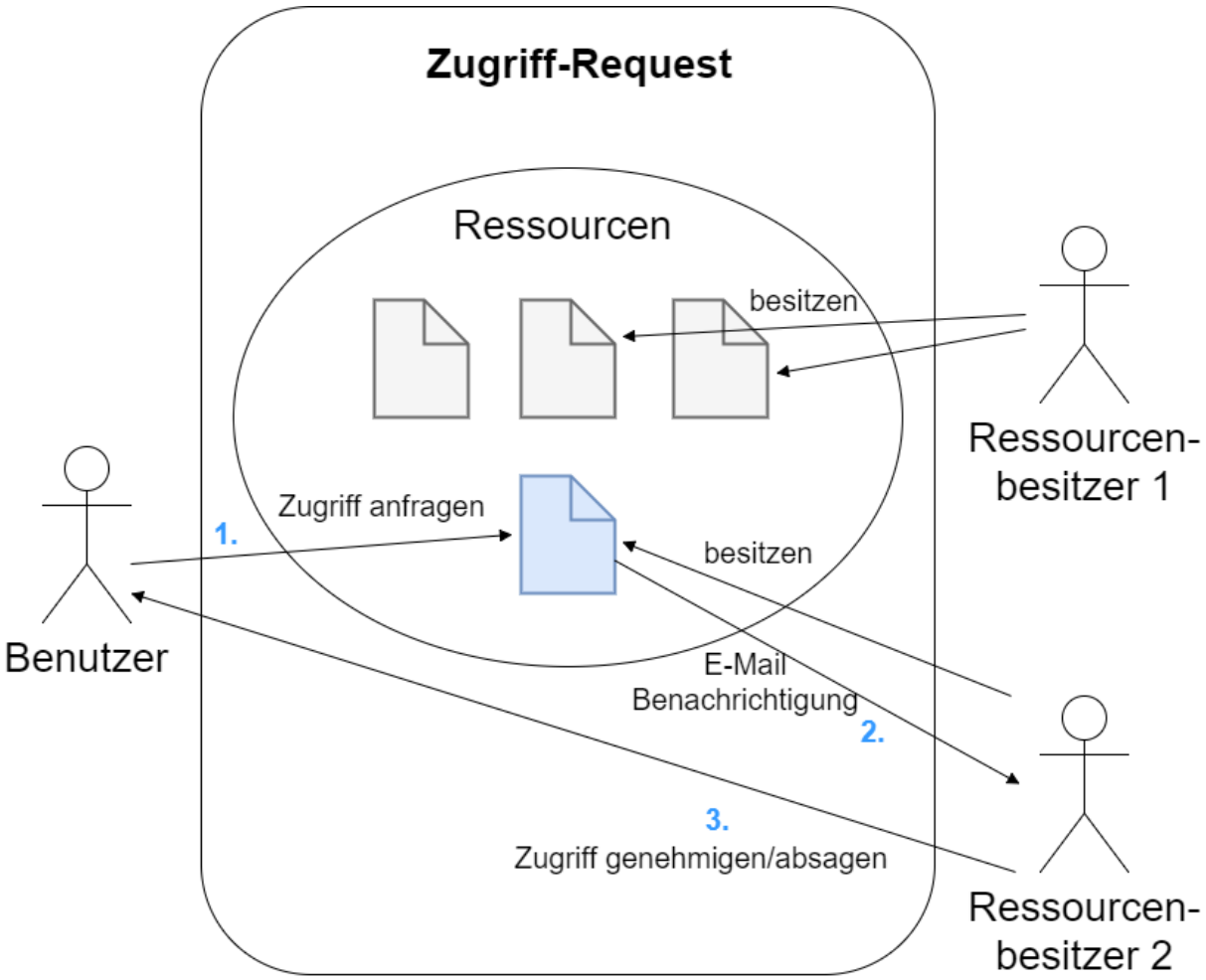
Nun möchte sie eine neue Ressource erstellen, darum klickt sie auf dem Knopf "Ressource hinzufügen". Später entscheidet sich Alice ihre neue Ressource X zu überprüfen. Sie sucht im Portal nach der Ressource X und findet sie. Weil sie der Besitzer ist, hat sie das Recht X zuzugreifen.



Zugriff-Request senden

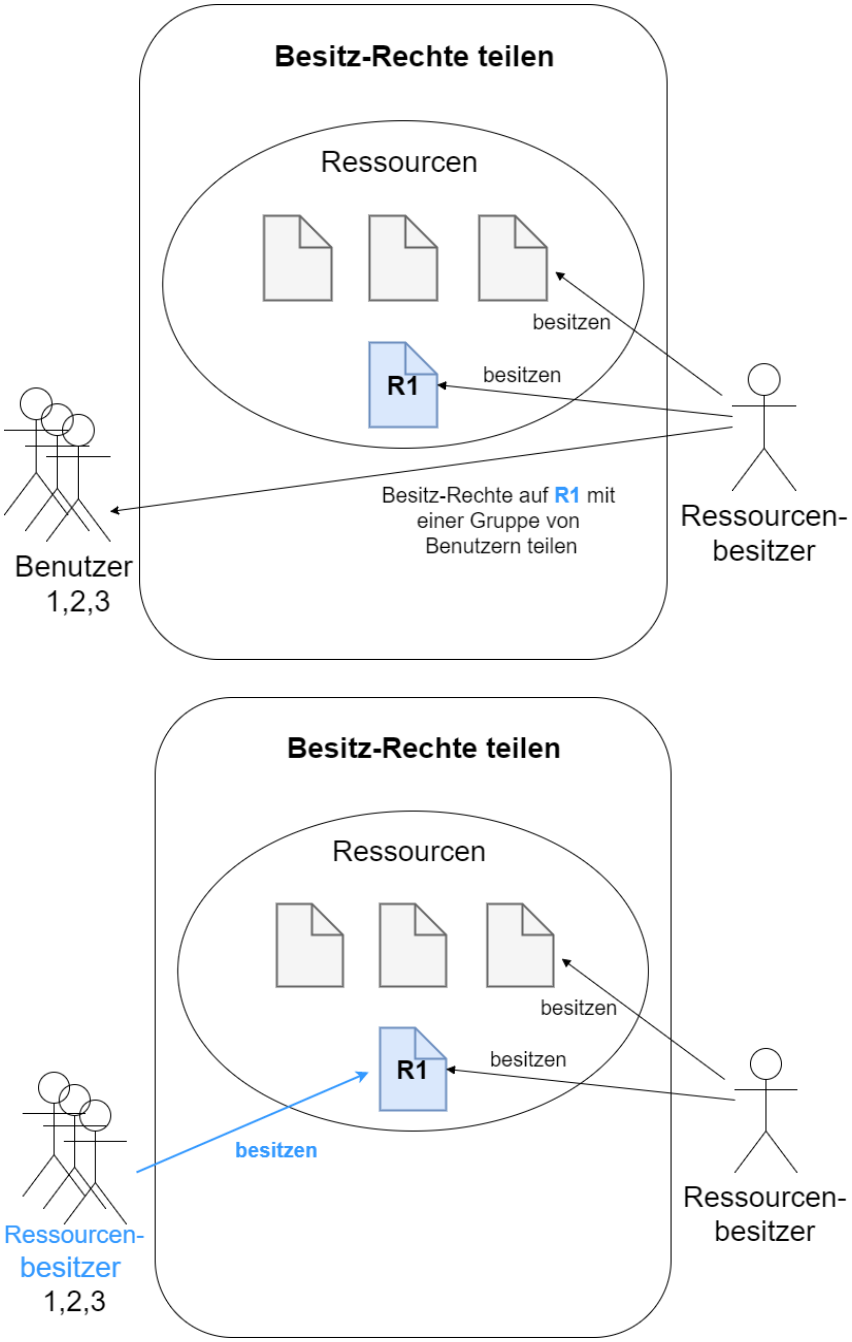
Bob hat Interesse an einer Ressource X im Portal von "V-FOR-WaTer:". Er probiert den Inhalt von X zuzugreifen. Leider hat er keine Zugriffsrechte darauf. Um solche Rechte zu bekommen, soll er ein Request am Besitzer von X senden, in diesem Fall - Alice. Bob wählt die Option "Zugriffsrechte anfragen".

Nach wenigen Sekunden bekommt Alice eine E-Mail-Benachrichtigung über das neue Request. Um zu entscheiden, ob sie die Zugriffsanfrage genehmigt, loggt sie sich im Portal ein. Dann sieht sie Bobs Anfrage und beschließt sie zu genehmigen. In kurzem bekommt Bob eine E-Mail mit der guten Neuigkeit. Nun kann er die Ressource zugreifen und ist glücklich.


Zugriff-Request
Ressourcen
besitzen
Ressourcen-
besitzer 1
Zugriff anfragen
1.
besitzen
Benutzer
E-Mail
Benachrichtigung
2.
3.
Zugriff genehmigen/absagen
Ressourcen-
besitzer 2

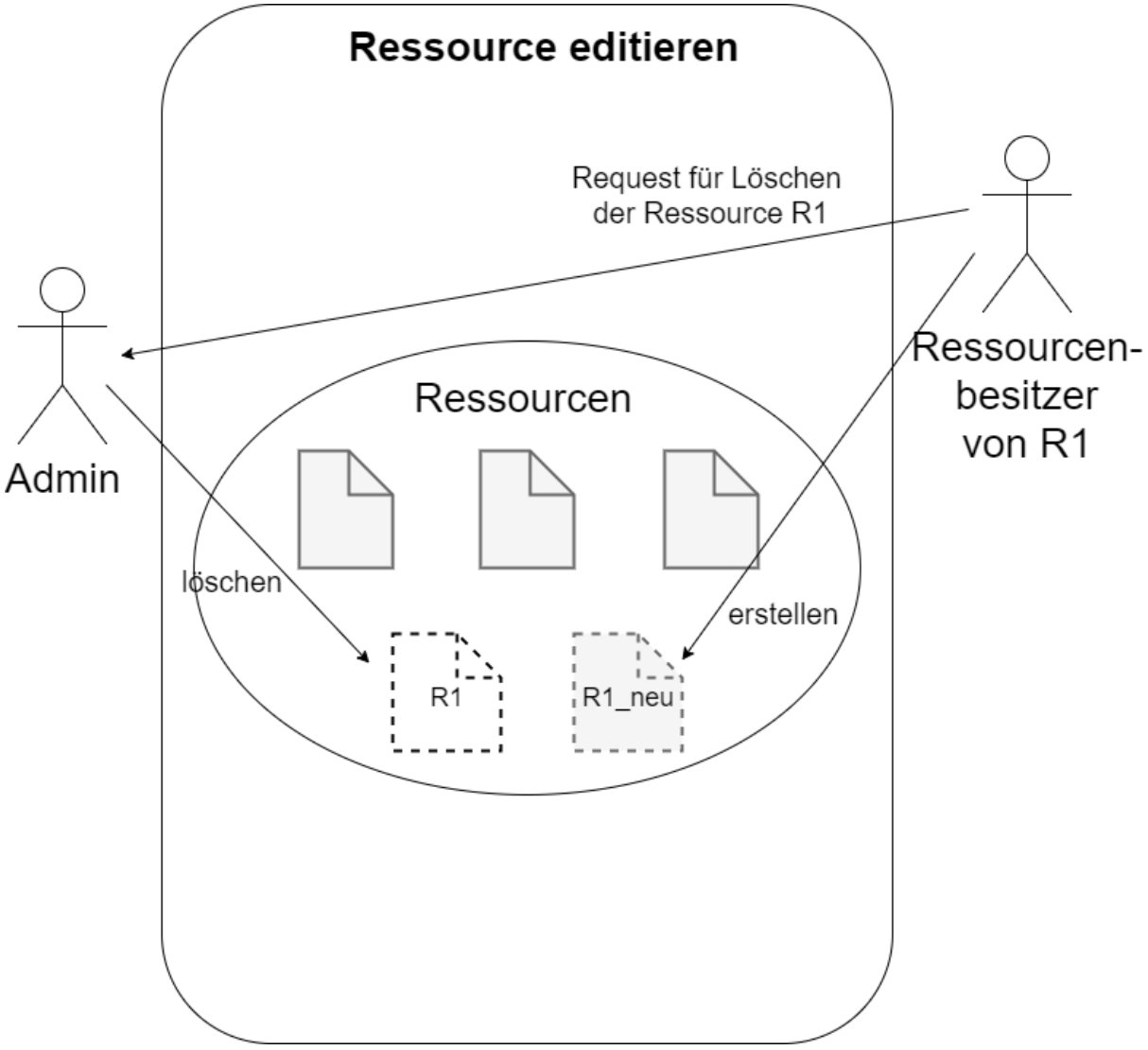
Besitz-Rechte teilen

Der Besitzer von Ressource Y, nämlich Bob, ist ein sehr beschäftigter Mann. Er hat keine Zeit und Lust jeden Tag die zahlreiche Zugriffsanfragen für Rechte auf Y zu beantworten. Deshalb hat er sich entschieden seine Besitz-Rechte mit drei Mitarbeitern von ihm zu teilen.
Er findet die Ressource Y und wählt die Option "Besitz-Rechte teilen". Dann findet er die Personen durch ihre Namen. Auf diese Weise kann jeder von der neuentstandene Gruppe von Besitzern eine zukünftige Zugriffsanfrage genehmigen oder ablehnen.



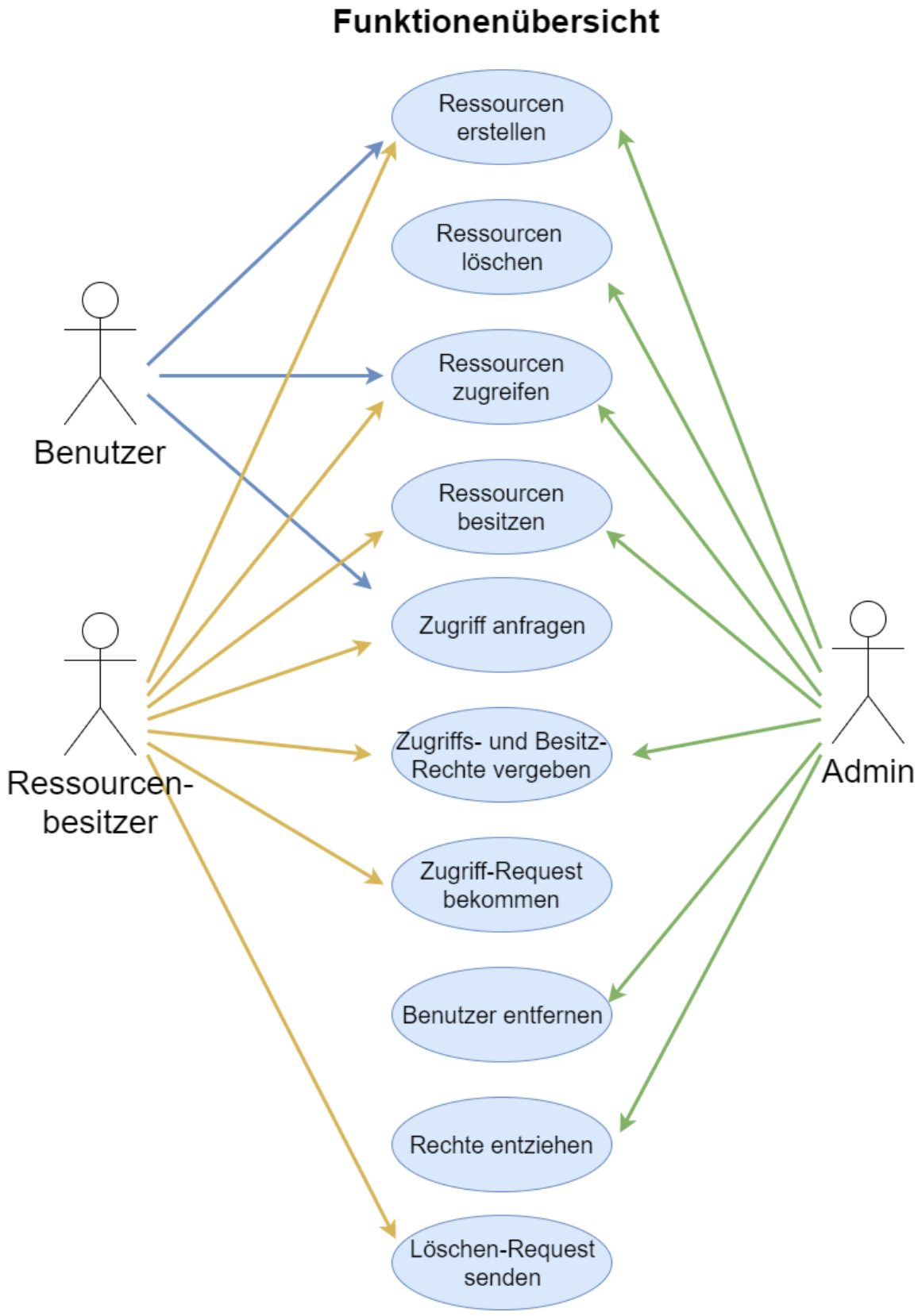
Ressource editieren

Alice hat ihre Meinung geändert und möchte jetzt etwas in Ressource X korrigieren. Da das Portal diese Option nicht anbietet, muss sie zuerst erneut die Ressource X erstellen. Dieses mal beinhaltet X aber auch die gemachte Korrektion. Danach sendet sie ein Löschen-Request am Administrator, damit er die alte Version von X zerstört.

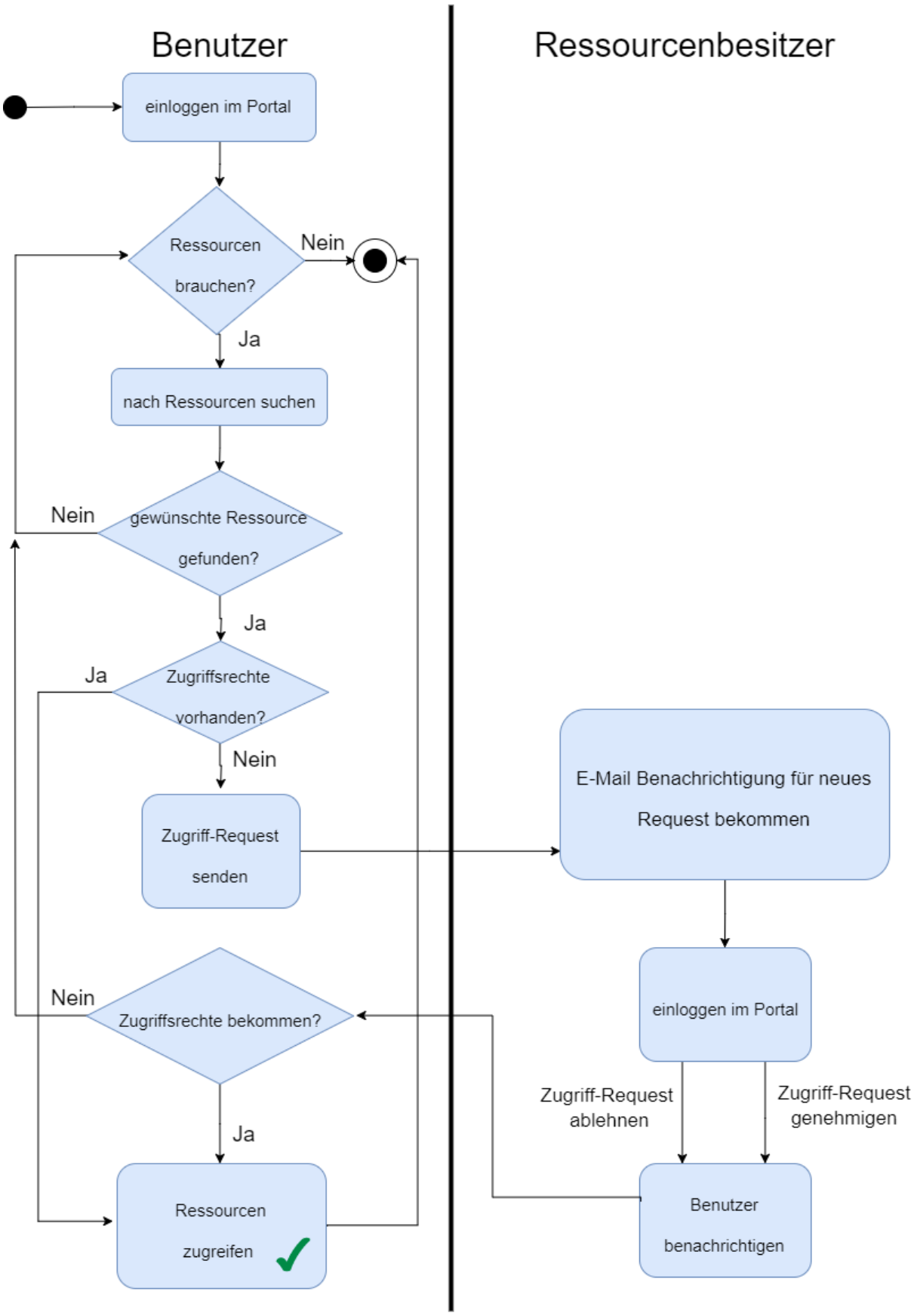


7.2 Diagramme

Funktionenübersichtsdiagramm

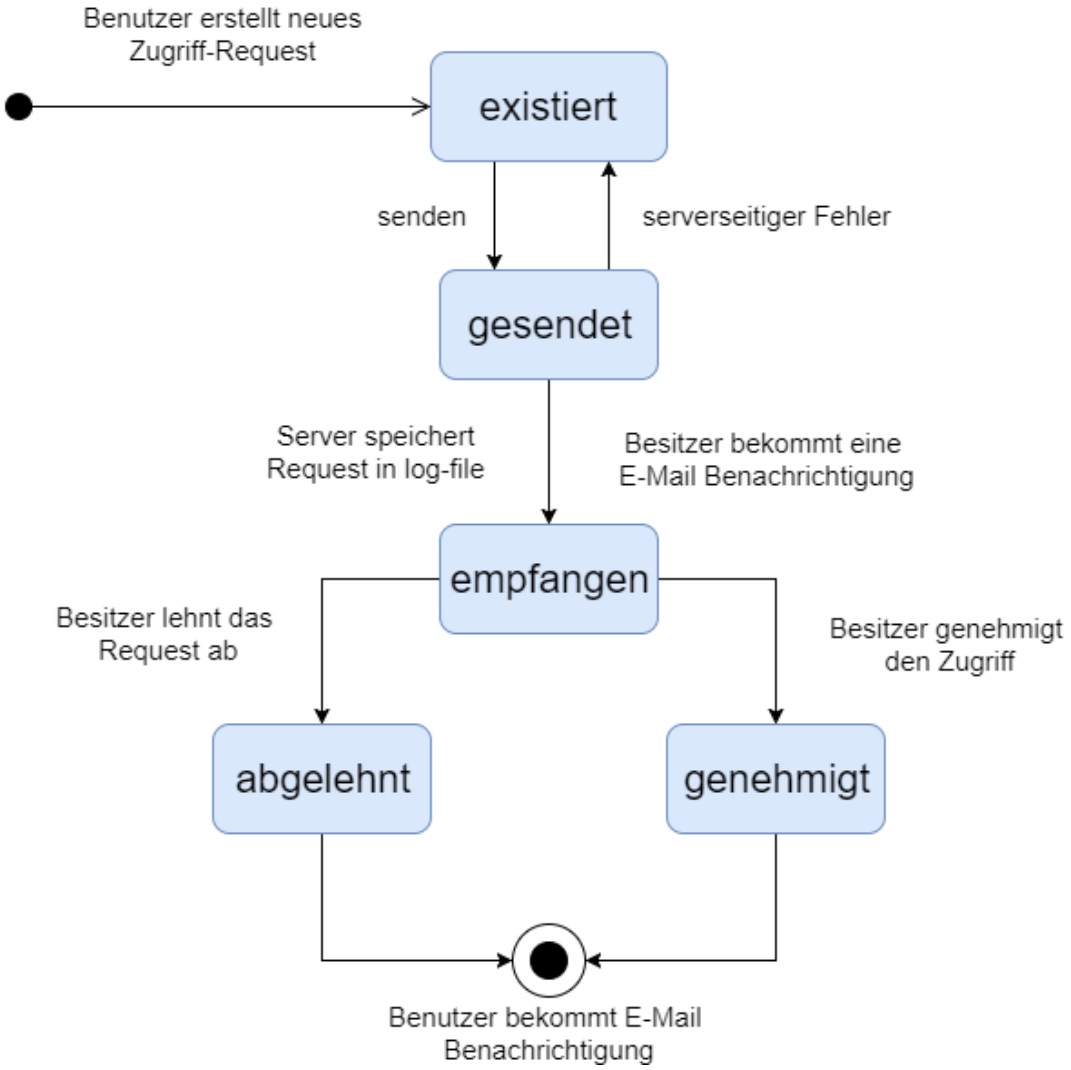


Kontrollflussdiagramm “Ressource zugreifen“



Zustandsdiagramm “Zugriff-Request“

Das Diagramm stellt die mögliche Zustände eines Zugriff-Requests dar, wenn ein Benutzer ohne Zugriffsrechte eine Ressource zugreifen will.



8 Qualitätsbestimmungen

Produktivität	**sehr wichtig**	**wichtig**	**normal**	**nicht relevant**
Funktionalität				
Angemessenheit		x		
Richtigkeit	x			
Interoperabilität	x			
Sicherheit		x		
Zuverlässigkeit				
Reife			x	
Fehlertoleranz				x
Wiederherstellbarkeit				x
Benutzbarkeit				
Verständlichkeit	x			
Erlernbarkeit		x		
Bedienbarkeit	x			
Effizienz				
Zeitverhalten			x	
Verbrauchsverhalten	x			
Änderbarkeit				
Analysierbarkeit				x
Modifizierbarkeit	x			
Stabilität		x		
Prüfbarkeit		x		
Benutzbarkeit				
Anpassbarkeit	x			
Installierbarkeit		x		
Konformität				x
Austauschbarkeit	x			

9 Globale Testfälle

9.1 Benutzertestfälle

/**T010**/ Profilseite öffnen. (/**F010**/)

/**T020**/ Namen ändern. (/**F020**/)

/**T030**/ Ressourcen öffnen. (/**F030**/)

/**T040**/ Neue Ressource erstellen. (/**F040**/)

/**T050**/ Request senden. (/**F050**/)

/**T060**/ Benachrichtigungen kontrollieren. (/**F060**/)

/**T070**/ Requestliste ansehen. (/**F070**/)

/**T080**/ Multiple Request senden. (/**F080**/)

/**T090**/ Administratorrechte anfragen. (/**F090**/)

/**T100**/ Token erstellen und validieren. (/**F100**/)

9.2 Administratortestfälle

/**T110**/ Request zum Löschen von einem Ressource zum Administrator senden. (/**F110**/)

/**T120**/ Ressource löschen. (/**F120**/)

/**T130**/ Zugriffsrechte zu einem Benutzer geben.(/**F130**/)

/**T140**/ Zugriffsrechte von einem Benutzer entziehen.(/**F130**/)

/**T150**/ Leserechte zu einem Benutzer geben.(/**F130**/)

/**T160**/ Leserechte von einem Benutzer entziehen.(/**F130**/)

/**T170**/ Löschen von Account und Daten, die zu einem Benutzer gehören.(/**F140**/)

/**T180**/ Adminrequest an den Administrator senden. (/**F150**/)

/**T190**/ Suchen nach einem Benutzer und ihn Blockieren . (/**F160**/,/**F170**/)

9.3 Ressourcenbesitzertestfälle

/**T200**/ Requestsliste kontrollieren.(/**F180**/)

/**T210**/ Liste von besessenen Ressourcen kontrollieren.(/**F190**/)

/**T220**/ Zugriffsrechte an anderen Benutzer vergeben.(/**F200**/)

/**T230**/ Request auf Zugriffsrechte ablehnen.(/**F210**/)

/**T240**/ Request auf Zugriffsrechte genehmigen.(/**F210**/)

/**T250**/ Besitzrechte an anderen Benutzer vergeben.(/**F220**/)

/**T260**/ Request zum Löschen von Ressource absenden.(/**F230**/)

/**T270**/ Löschbenachrichtigung kontrollieren.(/**F240**/)

/**T280**/ Zugriffsrechte einer Gruppe von Benutzern vergeben.(/**F250**/)

Glossar

Administrator: Ein Administrator ist der Verwalter des Systems, er unterstützt die Datenbankverwaltung und er hat im Vergleich zu Standardbenutzer erweiterte Rechte. Er spielt auch die Rolle der Moderator, damit er die Rechte zum Benutzer einräumen und entziehen kann. Der Administrator ist ein Mitarbeiter von V-FOR-WaTer.

Benutzer: Eine Person, die das Portal benutzt. Somit verfügt sie unter anderem über Profilinformationen, die auf dem Datenbank gespeichert sind.

Besitz-Rechte: Alle Rechte über die ein Ressourcenbesitzer verfügt. Besitz-Rechte implizieren Zugriffsrechte .

Datenbank: Eine Datenbank ist eine eine große Menge von Daten, die in einem Computer nach bestimmten Kriterien organisiert sind und komplexe Abfragen zulassen.

ID: (Abkürzung für Identifikator). Ein Identifikator (auch Kennzeichen) ist ein mit einer bestimmten Identität verknüpftes Merkmal zur eindeutigen Identifizierung des tragenden Benutzer .

Loeschen-Request: Ein Löschen-Request ist eine vom Ressourcenbesitzer zum Administrator gesendeter Request. Dieses Request entspricht dem Wunsch, eine oder mehrere Ressourcen zu löschen und wird negativ oder positiv beantwortet.

Meta-daten: Meta-daten oder Metainformationen sind strukturierte Daten, die Informationen über Merkmale anderer Daten enthalten .

Ressourcenbesitzer: Ein Ressourcenbesitzer ist ein Benutzer der eigenen Ressourcen erstellt hat.

Token Das Token ist eine textuelle Datei bestehend aus einem Verifizierungsstring.Im String sind die ID der Nutzer, seine Rechte auf die Ressourcen im Portal und die Gültigkeitsdauer des Tokens kodiert. plural.

V-FOR-WaTer: Die Virtuelle Forschungsumgebung für die Wasser- und Terrestrische Umweltforschung (V-FOR-WaTer) ist eine generische, virtuelle Forschungsumgebung für den gemeinsamen, systemischen Umgang mit Daten aus der Wasser- und Umweltforschung.

Web-Portal: Ein Web-Portal ist ein Anwendungssystem, das sich durch die Integration von Anwendungen, Prozessen und Diensten auszeichnet. Ein Portal stellt seinem Benutzer verschiedene Funktionen zur Verfügung, wie beispielsweise Navigation und Benutzerverwaltung. Außerdem koordiniert es die Suche und die Präsentation von Informationen und soll die Sicherheit gewährleisten.

Zugriffsrechte: Rechte den Inhalt einer Ressource zu lesen und auszuführen .