

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 Lese-Rechte hat.
- Der Benutzer kann ein Request dem Ressourcenbesitzer senden, um Lese-Rechte 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 ändern.

Ressourcenbesitzer

- Der Ressourcenbesitzer kann Lese-Rechte auf seine eigenen Ressourcen vergeben.
- Der Ressourcenbesitzer kann freiwillig seine Besitz-Rechte mit anderen Benutzern teilen.
- Der Ressourcenbesitzer kann ein Löschen-Request für seine eigenen Ressourcen dem Administrator senden.
- Der Ressourcenbesitzer kann den Name vom Request-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 Rechte auf Ressourcen beliebig vergeben (ohne selbst Ressourcenbesitzer zu sein).
 - Der Administrator kann Ressourcenbesitzer ändern.

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 Lese-Rechte 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 IDs von Benutzern sind nicht 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
 - Netzwerkfähig

4 Funktionale Anforderungen

Im Folgenden werden die funktionale Anforderungen: sowohl Musskriterien als auch Wunschkriterien erläutert. Die Nummern optionaler 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 Meta-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.

4.2 Administratorfunktionen

/F100/ Bekommen von Löschrequeste

Der Admin bekommt Requeste von einem Ressourcenbesitzer zur RessourcenLöschen.

Beschreibung:

- (1) Nachdem der Ressourcenbesitzer ein Löschrequest gesendet hat, werden alle Admins 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 Admin kann seine Entscheidung direkt von der Nachricht durch zwei Knöpfe "Ja" oder "Nein" treffen.

/F110/ Löschen von Ressourcen

Der Admin darf die Ressourcen im Portal löschen.

Beschreibung:

- (1) Die Löschen kann entweder durch die in /F060/ beschriebene Weise oder auch ohne Request passieren.
- (2) Nach der Löschen der Ressource werden alle Ressourcenbesitzer(eventuell auch alle Benutzer mit Leserechte, bei Publicressourcen problematisch) durch eine Email darüber informiert.

/F120/ Bekommen von Adminrequeste

Der Admin bekommt Requeste von einem Benutzer, der vom Admin verlangt, ein Admin zu werden.

/F130/ Löschen von Ressourcen

Der Admin darf Adminrechte einem anderen Benutzer geben.

4.3 Ressourcenbesitzerfunktionen

/F140/ Übersicht der Requests:

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

/F150/ Übergabe der Zugriffsrechte:

Der Besitzer kann Zugriffsrechte an anderen Benutzer vergeben.

/F160/ Request auf Zugriffsrechte ablehnen/genehmigen:

Der Ressourcenbesitzer kann die gesendeten Requests, die von anderen Benutzern zur Anforderung einer Zugriffsrechte gesendet wurden, entweder ablehnen oder annehmen. In beiden Fälle werden der entsprechenden Benutzern benachrichtigt. Im Fall Genehmigung bekommt der Benutzer Die Zugriffsrechte auf gewünschte Ressourcen.

/F170/ Übergabe der Besitz-Rechte:

Der Ressourcenbesitzer kann seine Besitz-Rechte mit anderen Benutzern teilen. In diesem Fall haben die anderen Benutzer dieselben Rechte, die Ressourcenbesitzer hat.

/F180/ Löschen-Request senden:

Der Ressourcenbesitzer ist in der Lage zum Löschen seinen Ressourcen ein Request dem Administrator zu senden.

/F190/ Löschbenachrichtigungen:

Beim Löschen einer Ressource werden allen Ressourcenbesitzer benachrichtigt.

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)

5.2.1 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 Benutzer-Funktionen

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.

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 Korrektur. 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“

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 und Testszenarien

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/)

9.2 Ressourcenbesitzertestfälle

- /T100/ Liste von besessenen Ressourcen kontrollieren.
- /T110/ Zugriffsrechte an anderen Benutzer vergeben.
- /T120/ Requestliste kontrollieren.
- /T130/ Request auf Zugriffsrechte ablehnen.
- /T140/ Request auf Zugriffsrechte genehmigen.
- /T150/ Besitzrechte an anderen Benutzer vergeben.
- /T160/ Request zum Löschen von Ressource absenden
- /T170/ Löschbenachrichtigung kontrollieren.

9.3 Administratortestfälle

- /T180/ bu
