Authentifizierungsservice für ShareIt

Autoren: Nico Daßler, Aykut Yilmaz, Julian Keppeler

1. Motivation

Die in der letzten Aufgabe erstellte Platform für das Teilen von Medien ist bisher sämtlichen Gefahren des Internets ausgeliefert (Trolle usw.). Deshalb benötigen wir ein Authentifizierungssystem um unsere Bücher und Discs vor den bösen Jungs zu schützen.

2. System: OAuth 2

Um zu verhindern, dass bei jeder Anfrage an den ShareIt Service oder andere Services ein neuer Authentifzierungsprozess angestoßen wird, arbeitet man mit einem Token, dass einen Client berechtigt auf den Service zuzugreifen.

Folgende Services werden für den Vorgang benötigt:

- Authentifizierungsservice
- Ressourcenservice

Hier ein Ablauf des Authentifizierungsvorgangs:

1) Der Client schickt einen Request an Authenfizierungsservice mit Nutzername + Passwort.
2) Der Server antwortet:
    1) Erfolgreich: Server sendet das Token.
    2) Fehler: Server sendet Fehlermeldung und kein Token.
3) Der Client kann nun mit dem Token auf den Ressourcenservice zugreifen, indem er das Token bei jeder Anfrage mitsendet.
4) Erhält der Ressourcenservice eine Anfrage mit Token, muss er dieses überprüfen. Hierfür schickt er eine Anfrage an den Authentifzierungsservice, welcher das Token verifziert.
5) Der Authentifzierungsservice antwortet:
    1) Erfolgreich: Token ist gültig.
    2) Fehler: Token ist ungültig.
6) Der Ressourcenserver erhält die Antwort und schickt eine Antwort an den Client:
    1) Token gültig: Anfrage vom Client wird beantwortet.
    2) Token ungültig: Anfrage vom Client wird nicht beantwortet.
7) Done Client is happy.

3. Beschreibung der Services

URL-Template	**Beschreibung**
/shareit/auth	Der Authentifizierungsservice. Dieser Service stellt eine Nutzername + Passwort Überprüfung zu Verfügung und sendet ein Token zurück. Für die Speicherung der Passwörter und Nutzernamen reicht es vorerst aus, diese statisch in eine Pseudo-Datenbank einzutragen. Außerdem muss er zugeschickte Tokens prüfen und melden ob diese gültig sind. Die Tokens können nach einer Weile ablaufen oder auch nicht. Das bleibt Ihnen überlassen. Überlegen Sie sich hierfür, wie die Tokens vom Server ausgeliefert werden, welche Form sie haben, wie sie im Client gespeichert werden sollen und wie sie dem Service Tokens zum Überprüfen schicken wollen.
/shareit/media	Der Ressourcenservice. Der in der letzten Praktikumsaufgabe implementierte Service. Der alte Service muss um die Authentifzierung erweitert werden. Überlegen Sie sich eine Möglichkeit um das Access-Token bei einer Anfrage mitzusenden. Beachten Sie dabei vor allem das gleichzeitige Senden des Tokens mit einem Buch oder einer Disc im Body.

4. Architektur

Verwenden Sie für den Authentifzierungsservice (wie auch in der letzten Aufgabe) ein Servlet um die Requests anzunehmen und zu verarbeiten. Verwenden Sie dabei eine ähnliche Architektur wie beim letzten Mal.
Nutzen Sie für die Implementierung Bibliotheken (Jackson, Jersey-Servlets usw.). Falls Sie geeignete Bibliotheken für die neu hinzugekommenen Funktionen finden und nutzen wollen, können Sie das tun. Eine Implementierung „von Hand“ ist allerdings auch in Ordnung, nimmt aber eventuell mehr Zeit in Anspruch.

5. Weiterführende Aufgaben

2 Personen:
Die oben beschriebenen Services müssen implementier bzw. angepasst werden.

3 Personen:
2 Personen + Erweitern Sie den Authentifizierungsservice, so dass er Registrierungsanfragen entgegennimmt und die neuen Nutzer in die Datenbank einträgt. Eventuell müssen die URL-Templates angepasst werden.

4 Personen:
3 Personen + Beschreibung der Verknüpfung von Exemplaren mit Nutzern. Wer hat welches Buch zur Verfügung gestellt und ausgehliehen?

6. Ende

Nun sind Sie gewappnet um es mit den Unholden aus dem Internet aufzunehmen. Viel Glück!