**Userverwaltung**

In dieser Aufgabe implementieren Sie eine Userverwaltung für ihre shareit-Anwendung.

Bitter erstellen Sie hierzu einen Authentication-Server (eine eigene API-Ressource), welche dies übernimmt.

Der Authentication-Server (z.B /api/v1/login) prüft zuerst per Basic-Auth die Zugangsdaten des Users und übergibt diesem danach einen sogenanntes „Statfull Session Cookie“.

Sie können dies ganz einfach mit Hilfe von curl (oder ihrem Browser) testen:

curl -c /tmp/cookie.–u user:password <https://url>/api/v1/login

Dies Authentifiziert sich über Basic-Auth an der genannten URL und speichert das Cookie im angegebenen Pfad (hier: /tmp/cookie.txt).

Bei darauf folgenden Abfragen wird die Basic-Auth dank des Cookies nicht mehr benötigt:

curl -c /tmp/cookie –b /tmp/cookie <https://url>

Nun wird das gespeicherte Cookie für jeden Request an den Server geschickt und geupdated falls etwas neues hinzu kommt.

Alle Ressourcen überprüfen die Identität und die des Users über dieses Cookie per API-Call an den Authentication-Server.

Die Verwaltung aller User und derer zugehörigen Cookies können Sie zur Vereinfachung als Liste implementieren.

Alle bisher genannten Aufgaben sind die Mindestanforderung für ein Team der Stärke 2.

Bei 3er Teams implementieren Sie bitte zusätzlich einen Timeout mit dessen Hilfe ein Cookie nach einer bestimmten Zeit ungültig wird.

Bei 4er Teams prüfen Sie bitte zusätzlich die Permissions des Users für eine einzelne API-Ressource.

Hierzu können Sie sich der Einfachheit halber wieder eine Liste definieren welche sämtliche User und die ihnen erlaubten API-Ressourcen abbildet.

Der Authentication-Server prüft mit dem Cookie nicht nur ob der User selbst überhaupt angemeldet ist, sondern auch ob dieser User Zugriff auf seine soeben genutzte API-Ressource hat.