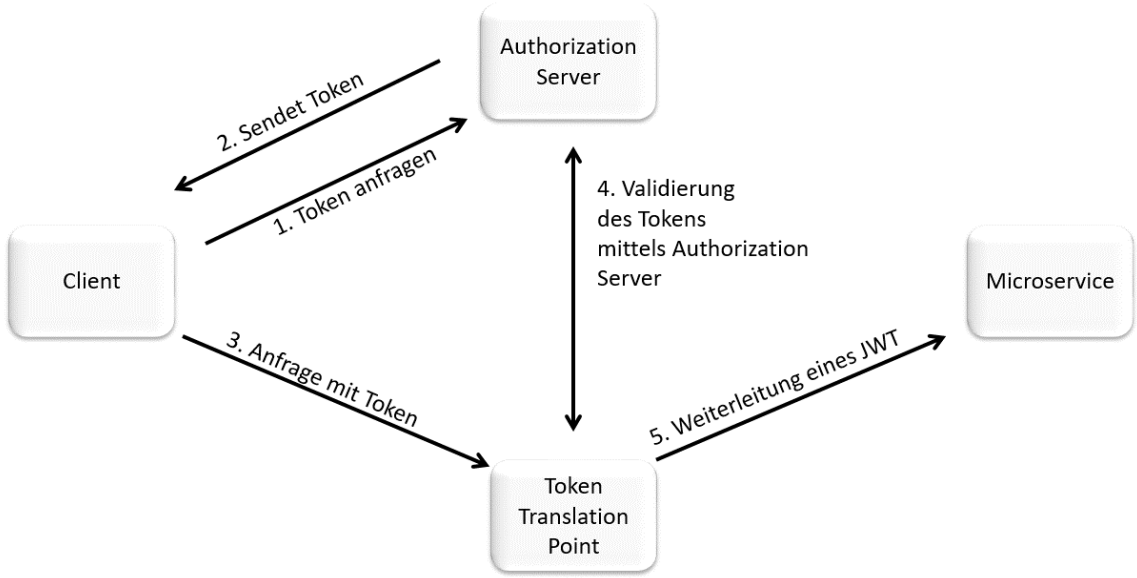
ShareIt Teil 2

Ausgangssituation

Nachdem Sie in ShareIt Teil 1 am Ende erfolgreich Ihren ersten Microservice deployed haben, geht es nun in der nächsten Aufgabe darum diesen zu erweitern. Momentan ist es der Fall das jeder auf Ihren Microservice zugreifen kann.
In diesem Praktikum wird es darum gehen, den Zugriff auf den Microservice zu limitieren und eine Identifikationsprüfung mittels OAuth, JSON Web Tokens (JWT) und einem Token Translation Point durchzuführen.

Übersicht



Anpassung Ihrer bisherigen Aufgabe

Da Sie ab sofort innerhalb Ihres Systems nur noch mit JSON Web Tokens arbeiten müssen sie als erstes Anpassungen an ihrem bisherigen Microservice vornehmen.

Implementierung des Token Translation Point/Reverse Proxy

Nun gilt es einen Token Translation Point/Reverse Proxy zu implementieren welcher vom Client ein Token erhält und dieses dann mittels des Authorization Servers validiert und anschließend ein JSON Web Token erzeugt.
Ihr Microservice erhält nun dieses JWT um mit der Verarbeitung fortzufahren.
Durch diese Implementierung garantieren Sie, dass der Client keine Benutzerspezifischen Daten besitzt, jedoch Ihr Microservice die benötigten Daten vorliegen hat.

Authorization Server

Als Authorization Server sollten Sie, um sich die Aufgabe etwas zu erleichtern, auf einen bereits implementierten Dienst zurückgreifen.
Beispielsweise könnten Sie hierbei auf den OAuth2 Service von Heroku zurückgreifen.

Zusatz Aufgabe für Gruppen mit 3+ Studenten

Da Sie bereits die Anlage von Exemplaren implementiert haben müssen Sie auch für diese, obige Anpassungen durchführen.
Trennen Sie zusätzlich den Microservice der Medien und der Exemplare und stellen Sie eine funktionierende Kommunikation her.