LU05d - JSON Web Token (JWT)

Siehe auch JSON_Web_Token und jwt.io

JSON Web Token sind eine standardisierte Methode um sichere Daten zwischen Client und Server auszutauschen. Sie eignen sich unter anderem für die Authentifikation in stateless Webservices (z.B. RESTful Webservices) und verteilten Systemen.

Authentifikation mit JWT

1. Login

1. Der Client sendet einen Request mit Benutzername/Passwort an den Authenfikations-Service.
2. Der Service prüft Benutzername/Passwort erfolgreich ⇒ Der Benutzer ist angemeldet.
3. Der Service erzeugt ein Token mit den Angaben zum Benutzer wie
   - Benutzer-ID
   - Rolle
   - ...
4. Dieses Token wird verschlüsselt und signiert, bevor es an den Client gesendet wird.

Beispiel eines Tokens

In diesem Beispiel wird die eindeutige Kennung (uuid) des Benutzers und seine Rolle im Token gespeichert. Die Signatur des Tokens wurde mittels RSA mit SHA-256 eingesetzt (RS256).

```
{
  "alg": "RS256",
  "typ": "JWT"
}
{
  "uuid": "a6c162b8-fa10-4cdb-930a-f2d08dd821f3",
  "role": "admin"
}
```

2. Autorisation prüfen

1. Der Client sendet einen Request an den Book-Service um die Bücherliste zu lesen.
   Beim Request sendet der Client das Token mit, welches er beim erfolgreichen Login erhalten hat.
2. Der Server empfängt das Token, entschlüsselt es und prüft die Signatur.

Falls die Signatur korrekt ist, handelt es sich um ein legitimes Token.
3. Der Server kann nun anhand der Angaben im Token prüfen, ob der Client für den gewünschten Server autorisiert ist.

Sicherheit

Wie alle Daten die an den Client gesendet werden, können auch JSON Web Token gelesen und manipuliert werden. Die Sicherheit des Tokens wird durch das Verschlüsseln und Signieren der Daten erreicht.

- Die Verschlüsselung verhindert das Auslesen der Daten im Token durch einen Angreifer.
- Die Signatur dient zur Erkennung von Manipulationen am Token.

Umsetzung

Für die Umsetzung stehen eine Reihe von fertigen Bibliotheken zur Verfügung. Eine aktuelle Liste finden Sie auf der Seite von https://jwt.io/.

M321-LU05