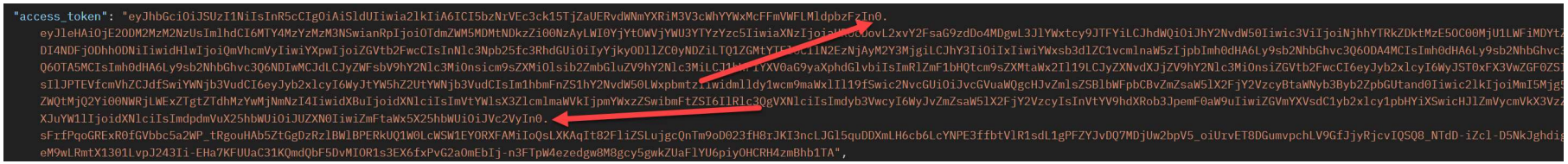
JWT mit Keycloak

Eine (sehr) kurze Einführung

Aufbau Token

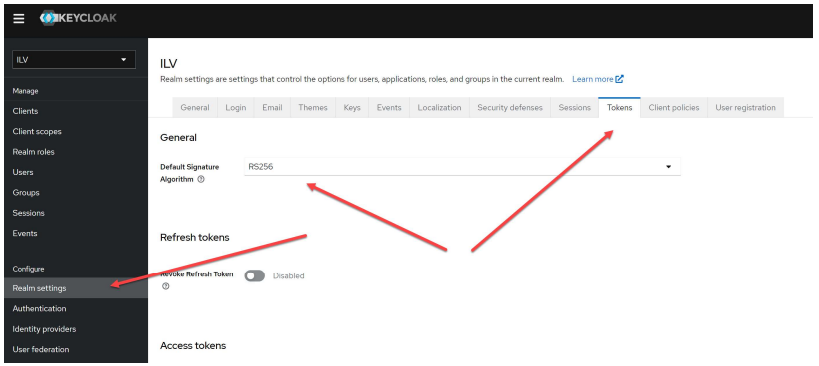
- Ein Token besteht aus 3 Teilen:
  - Header
  - Payload
  - Signatur
- Teile werden durch Punkte voneinander getrennt



- Achtung: Ein Token ist **NICHT** verschlüsselt –geheime Informationen haben nichts im Token zu suchen!

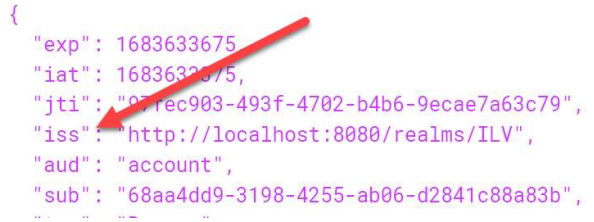
Erstellung Token

- Das Token wird von Keycloak erstellt
- Häufigste Algorithmen für Signatur
  - **RS256 (Private – Public Key Verfahren, asymmetrisch)**
  - HS256 (Secret)
- Wir verwenden RS256, nur der Inhaber des Private Keys (Keycloak) kann eine gültige Signatur erzeugen.



Überprüfung Token

- Hilfreiche Webseite für Betrachtung Token: https://jwt.io
- Keycloak Realm Informationen: http://localhost:8080/realms/ILV/.well-known/openid-configuration
- Keycloak Issuer: http://localhost:8080/realms/ILV
- Empfänger eines Tokens (z.B. Spring Backend) überprüft:
  - Signatur mit Public Key
  - Aussteller
  - Ablaufdatum
- Link zum Public Key ist im Token (Issuer) enthalten



Zusammenfassung

- Nur Keycloak kennt den Private Key und kann somit Signaturen erstellen.
- Im Token ist der Issuer enthalten (= URL zum Public Key)
- Der Konsument überprüft die Signatur mit dem Public Key und stellt die Gültigkeit (Ablaufdatum) sicher.
- Das Token selbst ist nicht verschlüsselt und kann von jedem gelesen werden.