# Externe und applikationsinterne Autorisierung in OAuth2 Systemen

## Gliederung

1. Einleitung
2. Technische Grundlagen
    a. Erklärung grundlegender Begriffe
        i. Authentifizierung
        ii. Autorisierung
        iii. Integrität
        iv. Authentizität
        v. Validierung
    b. OAuth2
        i. Rollen in OAuth2
            1. Resource Owner
            2. Resource Server
            3. Client
            4. Authorization Server
        ii. Erhalt von Token
            1. Authorization Code Grant
            2. Refresh Token
    c. Rivest–Shamir–Adleman (RSA)
    d. JSON Web Token (JWT)
        i. JSON Web Key (JWK)
        ii. JSON Web Signatur (JWS)
            1. RS256
    e. OpenID Connect
        i. ID Token
        ii. Authorization Code Grant
    f. OAuth2 Endpunkte des Autorisationsservers
        i. Authorization Endpunkt
        ii. Token Endpunkt
        iii. JSON Web Key Set (JWKS) Endpunkt
    g. Zugriffskontrolle
        i. Role Based Access Control (RBAC)
        ii. Attribute Based Access Control (ABAC)
3. Inhalt
    a. Systemarchitektur
        i. Authorization Server Keycloak
        ii. Postman
        iii. Spring Boot
        iv. Spring Security

1. OAuth2 Resource Server
2. Access Decision Manager

v. Open Policy Agent (OPA)
vi. Testsystem 1: Autorisierung in Ressourceserver
vii. Testsystem 2: Autorisierung entkoppelt von Ressourceserver mit Open Policy Agent (OPA)

b. Tests und Testtools
   i. Erhalt eines Tokens durch „Authorization Code Grant“ mit Postman
   ii. Apache JMeter
      1. Testplan Performanz
         a. Anzahl Threads über Zeitraum X
         b. HTTP-Request Header mit Token
         c. Listener für Protokollierung von Testergebnissen
            i. Graphische Darstellung der Round Trip Time
            ii. Statistische Protokollierung der Round Trip Time (Median, Mittelwert, Abweichung, Minimum, Maximum) und Datendurchsatz
      2. Testplan Performanz 2
         a. Ansteigende Anzahl Threads über Zeitraum X
         b. Listener für Protokollierung von Testergebnissen
            i. Graphische Darstellung der Round Trip Time
            ii. Berechnung der Steigung aus Grafik
      3. Testplan Last
         a. Maximale Anzahl Threads über Zeitraum X
         b. HTTP-Request Header mit großem Token
   iii. Windows Ressource Monitor

4. Experimente
   a. Auswertung
      i. Apache JMeter Auswertung „Testplan Performanz 1“
         1. Median, Mittelwert, Abweichung, Minimum, Maximum, Schwankung der RTT
         2. Datendurchsatz
      ii. Apache JMeter Auswertung „Testplan Performanz 2“
         1. Auswertung der Steigungen
      iii. Apache JMeter Auswertung „Last“
      iv. Windows Ressource Monitor
         1. CPU-Auslastung
         2. RAM-Belegung
5. Stand der Technik (Related Work) / Ausblick
   a. Neue Spezifikation für feinkörnige Autorisierung in OAuth2 in Arbeit - „OAuth 2.0 Rich Authorization Requests“
6. Zusammenfassung