OAuth und OpenID Connect im .NET-Technologie-Stack

Einführung in die Standards und praktische Umsetzung

Einleitung

- Ziele
  - Server implementieren
  - Abläufe verstehen
  - Möglichkeiten & Grenzen der Verfahren
- Motivation
  - Eigene Erfahrung
  - Missverständnisse
  - Relevanz

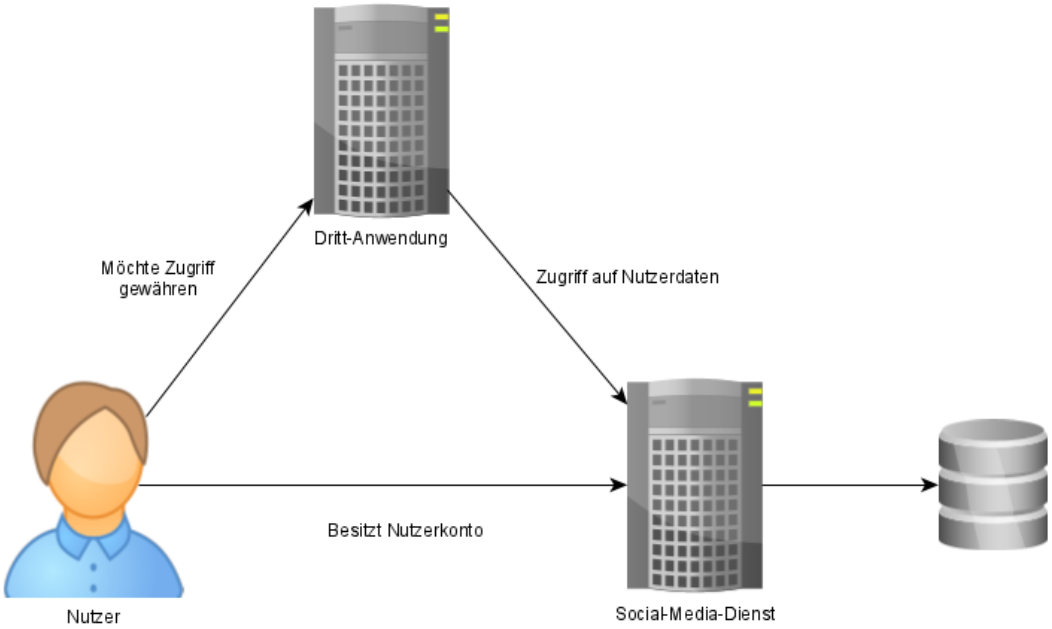
Aufbau

1. Einführung in Verfahren
   - OAuth2.0
   - OpenID Connect
2. Konkrete Technologien
   - IdentityServer4
   - ASP.NET Core MVC
3. Live Coding
   - Server
   - Client
   - Ressourcen-Server

OAuth2.0

EINFÜHRUNG

Problemfall



Probleme

- Anwendung agiert als Nutzer
  - Hat alle Rechte des Nutzers
  - Berechtigung entziehen
- Sicherheit
  - Passwort im Klartext
  - Passwort an mehreren Stellen gespeichert
  - Kompromittierung wirkt auf alle Beteiligen

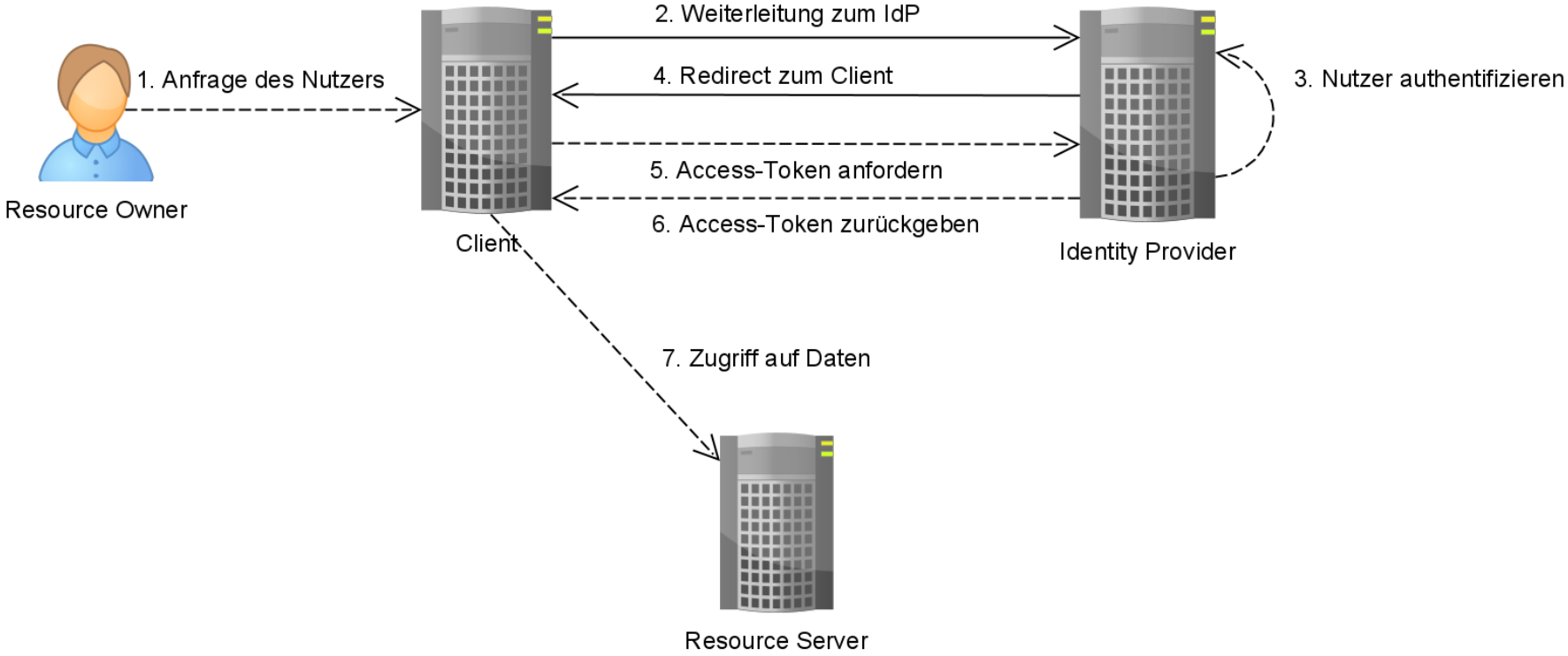
Lösung

- Trennung von User und Third Party Application
  - Anwendung ist dem Identity Provider bekannt
  - API-Berechtigungen gesondert verwaltet
  - Token als Schlüssel zu Ressourcen

Terminologie

- Resource Owner (User)
- Client (Third Party Application)
- Ressource Server
- Identity Provider
- Access Token
- Claims
- Scopes

Ablauf


1. Anfrage des Nutzers
2. Weiterleitung zum IdP
3. Nutzer authentifizieren
4. Redirect zum Client
5. Access-Token anfordern
6. Access-Token zurückgeben
7. Zugriff auf Daten
Resource Owner
Client
Identity Provider
Resource Server

Problem

- Keine Nutzerinformationen vorgesehen
- Betreiberspezifische
  - Erweiterungen
  - Endpunkte

OpenID Connect

- Führt Identity Token ein
- Schnittstellen zum Abruf von Nutzerdaten
- Discovery-Dokument
- Standardfelder für Informationen über Nutzer
- Zusätzlicher Flow → Hybrid Flow

Technologie

IDENTITY SERVER

Identity Server

- Open Source & kostenlos
- Provider-Bibliothek
- Häufige Verwendung
- Schulungen, Support & weitere kostenpflichtige Produkte
- Guter Datenbank-Support
- Gute Dokumentation

Live-Coding

- Aufsetzen dreier Template-Projekte
  - IdentityServer4
  - Client-Anwendung
  - Anwendung für den Zugriff auf Daten
- Einrichtung des Users und Clients (In-Memory)
- Zugriff auf gesicherte Daten der Drittanwendung

Vielen Dank!

W3L AG
info@w3l.de

2020