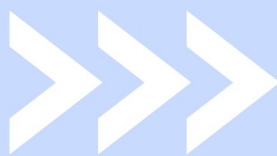


# OAuth Autorizacijski Sustav



- **OAuth je otvoreni standardni protokol za autorizaciju.**
- **Omogućuje aplikacijama trećih strana ograničeni pristup korisničkim resursima bez izlaganja vjerodajnica.**
- **Sve se više koristi za web i cloud usluge.**

## KLJUČNI KONCEPTI OAUTH 1.0

### ULOGE

- Korisnik: Vlasnik podataka, može odobriti pristup
- Klijent: Aplikacija koja traži pristup korisničkim podacima
- Pružatelj usluga: Server koji pohranjuje korisničke podatke i može rukovati zahtjevima za tokenima

### KORACI AUTORIZACIJE

- Klijent traži token zahtjeva od pružatelja usluga
- Korisnik autorizira token zahtjeva
- Klijent mijenja autorizirani token zahtjeva za pristupni token

### TOKENI

- Token zahtjeva: Privremena vjerodajnica za dobivanje korisničke autorizacije
- Pristupni token: Vjerodajnica za pristup korisničkim podacima, dobiva se nakon autorizacije

### POTPISI

- Osiguravaju integritet i autentičnost zahtjeva korištenjem HMAC-SHA1, RSA-SHA1 ili PLAINTEXT

## OAuth 2.0

### PREDNOSTI

- Pojednostavljena implementacija
- Bolja podrška za mobilne uređaje
- Fleksibilnost i prilagodljivost različitim slučajevima upotrebe

### NEDOSTATCI

- Oslanja se na HTTPS za sigurnost
- Nije unatrag kompatibilan s OAuth 1.0

## OAuth 1.0

### PREDNOSTI

- Povećana sigurnost korištenjem tokena umjesto lozinki
- Omogućuje ograničen pristup resursima
- Standardizirani protokol

### NEDOSTATCI

- Složena implementacija
- Zahtijeva kriptografske potpise
- Ograničena podrška za mobilne uređaje

## KLJUČNI KONCEPTI OAUTH 2.0

### ULOGE

- Korisnik: Autorizira aplikaciju za pristup resursima
- Klijent: Aplikacija koja traži pristup
- Autorizacijski server: Izdaje pristupne tokene nakon uspješne autentifikacije korisnika
- Poslužitelj resursa: Pohranjuje zaštićene resurse i prihvata pristupne tokene

### TOKENI

- Pristupni tokeni: Koriste se za pristup zaštićenim resursima
- Tokeni za osvježivanje: Koriste se za dobivanje novih pristupnih tokena

### VRSTE AUTORIZACIJE

- Token zahtjeva: Privremena vjerodajnica za dobivanje korisničke autorizacije
- Pristupni token: Vjerodajnica za pristup korisničkim podacima, dobiva se nakon autorizacije

### KRAJNJE TOČKE

- Krajnja točka autorizacije: Autentifikacija i autorizacija korisnika
- Krajnja točka tokena: Razmjena autorizacijskog odobrenja za tokene
- Krajnja točka preusmjeravanja: Preusmjeravanje korisnika nakon autorizacije



## SIGURNOSNI ASPEKTI OAUTH 2.0

- Korištenje HTTPS-a za sve komunikacije.
- Implementacija snažnih tokena.
- Redovita rotacija ključeva i tokena.
- Sigurno pohranjivanje tajni.
- Praćenje i revizija svih događaja autorizacije i autentifikacije.

## SIGURNOSNI ASPEKTI OAUTH 2.0

- **TLS:** Osigurava povjerljivost, integritet i autentičnost.
- **Sigurnost tokena:**
  - Zaštita tokena tijekom prijenosa i pohrane.
  - Korištenje sigurnih komunikacijskih kanala.
  - Enkripcija tokena.