

## 2. Autentisering

APIet bruker OAuth2 med **Client Credentials**-flyten. Du henter et JWT fra token-serveren og sender det med i alle API-kall.

### Hente token

Send en POST til `https://<miljø>/token-server/oauth/token` med følgende:

- Header: `Authorization: Basic <base64(clientId:clientSecret)>`
- Header: `Content-Type: application/x-www-form-urlencoded`
- Body: `grant_type=client_credentials`

Base64-strengen lager du ved å enkode `clientId:clientSecret` – kolon mellom, ingen mellomrom.

Eksempel på respons:

```
{
  "access_token": "eyJhbGciOiJI...\"",
  "token_type": "Bearer",
  "expires_in": 3600
}
```

### Bruke token

Send tokenet som `Authorization`-header i alle API-kall:

`Authorization: Bearer <access_token>`

### Tokenfornyelse

Tokenet utløper etter `expires_in` sekunder (typisk 3600 = 1 time). Implementer én av følgende strategier:

- **Proaktiv** – hent nytt token like før det utløper basert på `expires_in`
- **Reaktiv** – hent nytt token automatisk ved 401 `Unauthorized`-respons