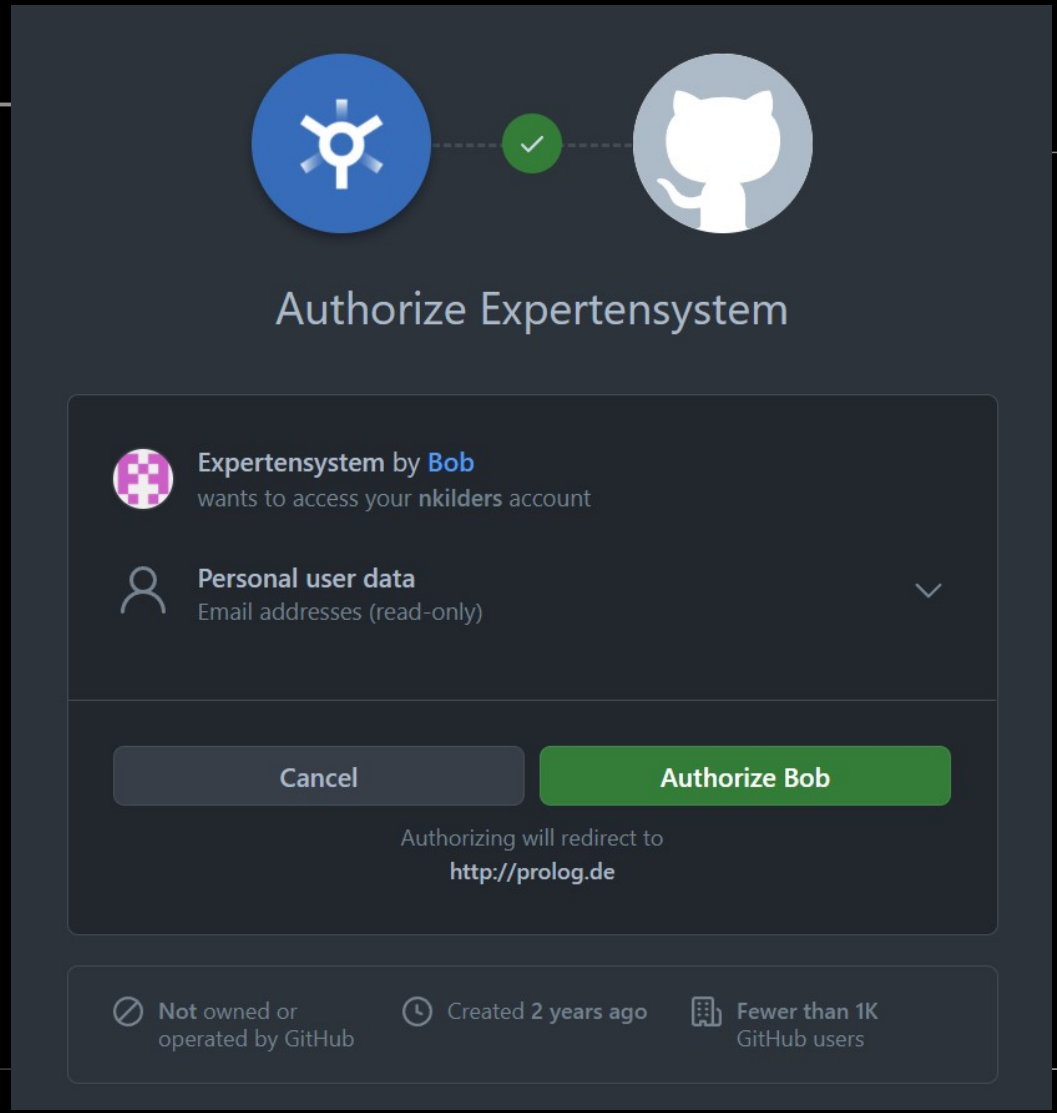
OAuth 2.0

Noah Kilders

Agenda

- OAuth
- Roles
- Tokens
- Scopes
- Flows

OAuth


Authorize Expertensystem
Expertensystem by Bob
wants to access your nkilders account
Personal user data
Email addresses (read-only)
Cancel
Authorize Bob
Authorizing will redirect to
http://prolog.de
Not owned or operated by GitHub
Created 2 years ago
Fewer than 1K GitHub users

OAuth

- „Open Authorization“
- Token-basiert
- 2012: 2.0
- IETF: RFC 6749

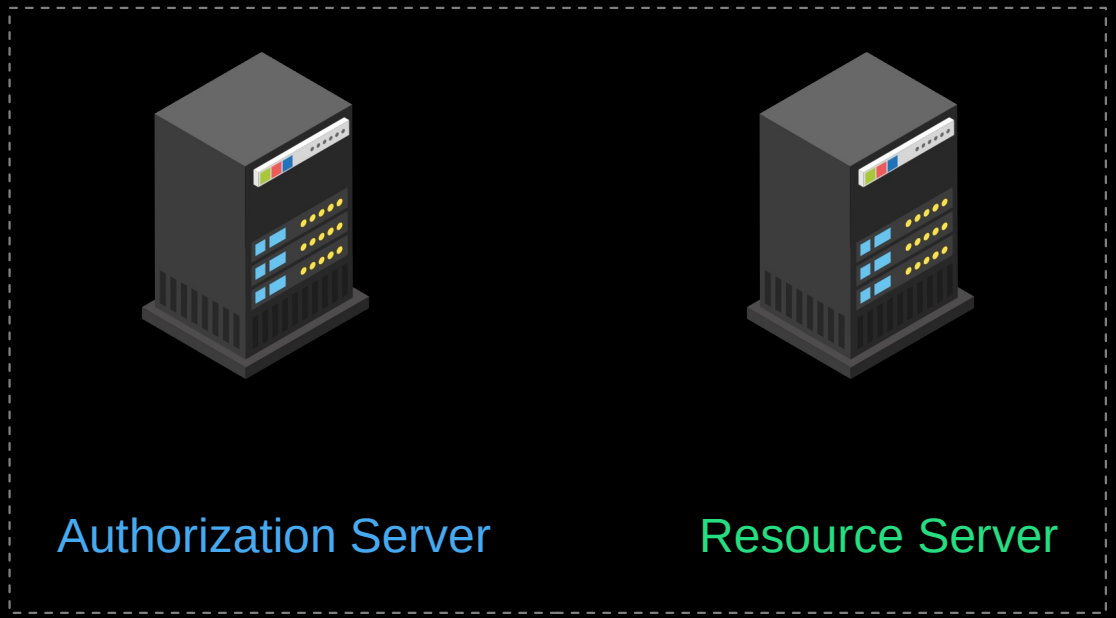
Roles

Application

„Bob“

Roles

Third Party Application



Roles

User / Resource Owner

„Alice“ / „Robo Alice“

Tokens

- Access Token
  - Für Zugriff auf Ressourcen
  - Kurzlebig
- Refresh Token
  - Um neuen Access Token zu erhalten
  - Langlebig

Scopes

- Zugriffsberechtigungen
- Limitieren Access Token

Flows

Application

Name
Scopes
Callback URL

Client ID
Client Secret

Authorization Server

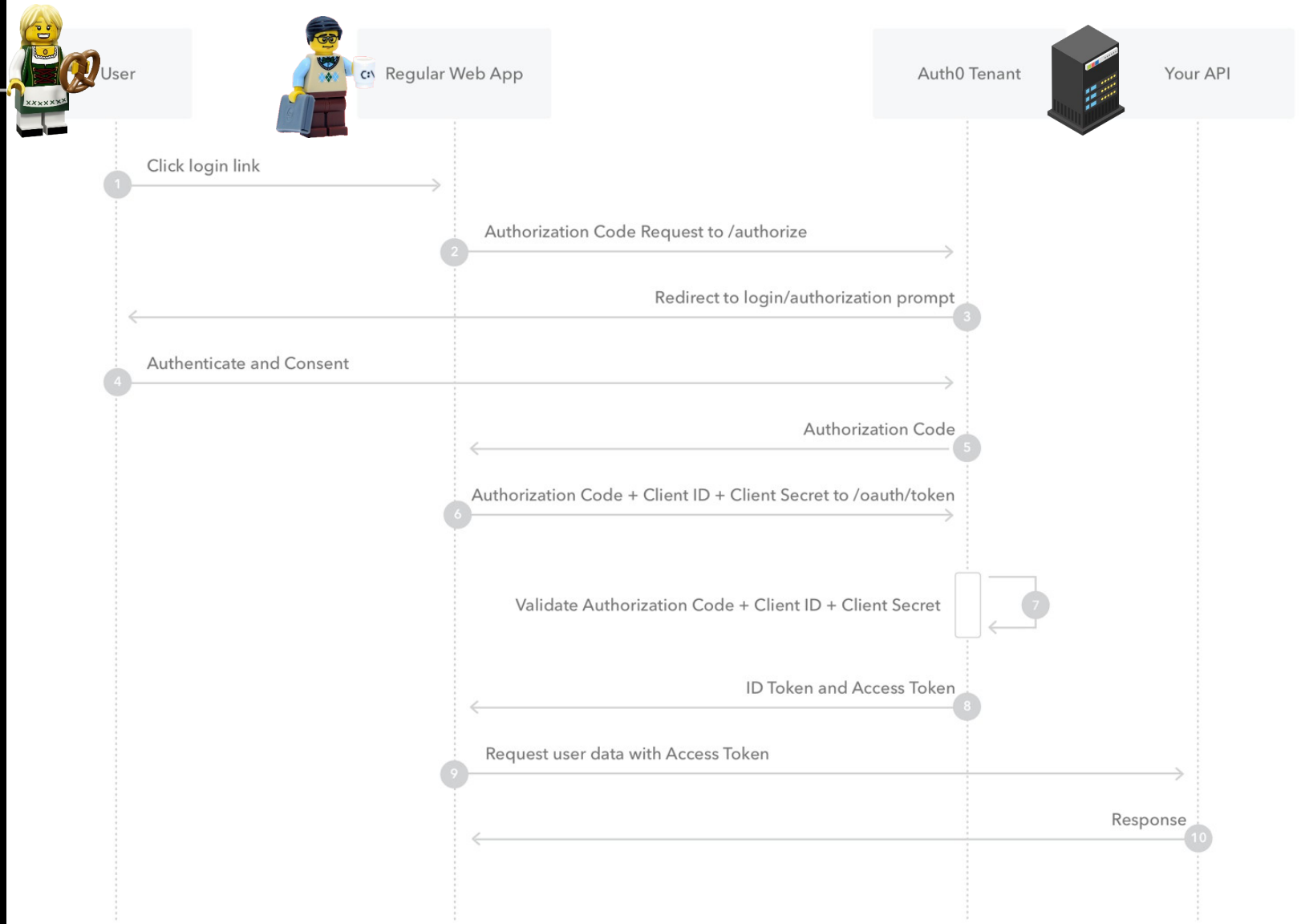
Flows

- Authorization Code Flow
- Client Credentials Flow
- Resource Owner Password Flow
- Implicit Flow

Authorization Code Flow

- Für serverseitige Apps
- Refresh Token möglich

Authorization Code



Client Credentials Flow

- Machine-to-machine (M2M) Apps
- App ist Resource Owner
- Refresh Token möglich, aber nicht empfohlen

Client Credentials

M2M App

Auth0 Tenant

Your API

1 Authenticate with Client ID + Client Secret to /token

2 Validate Client ID + Client Secret

3 Access Token

4 Request data with Access Token

5 Response

Resource Owner Password Flow

- Nutzung nicht empfohlen
- Für hoch vertrauenswürdige Apps
- App kann Username + Passwort sehen
- Refresh Token möglich

Resource Owner PW

User

Regular Web App

Auth0 Tenant

Your API

1 Click login link

2 Authenticate with Username + Password to /oauth/token

Validate Username + Password 3

4 Access Token

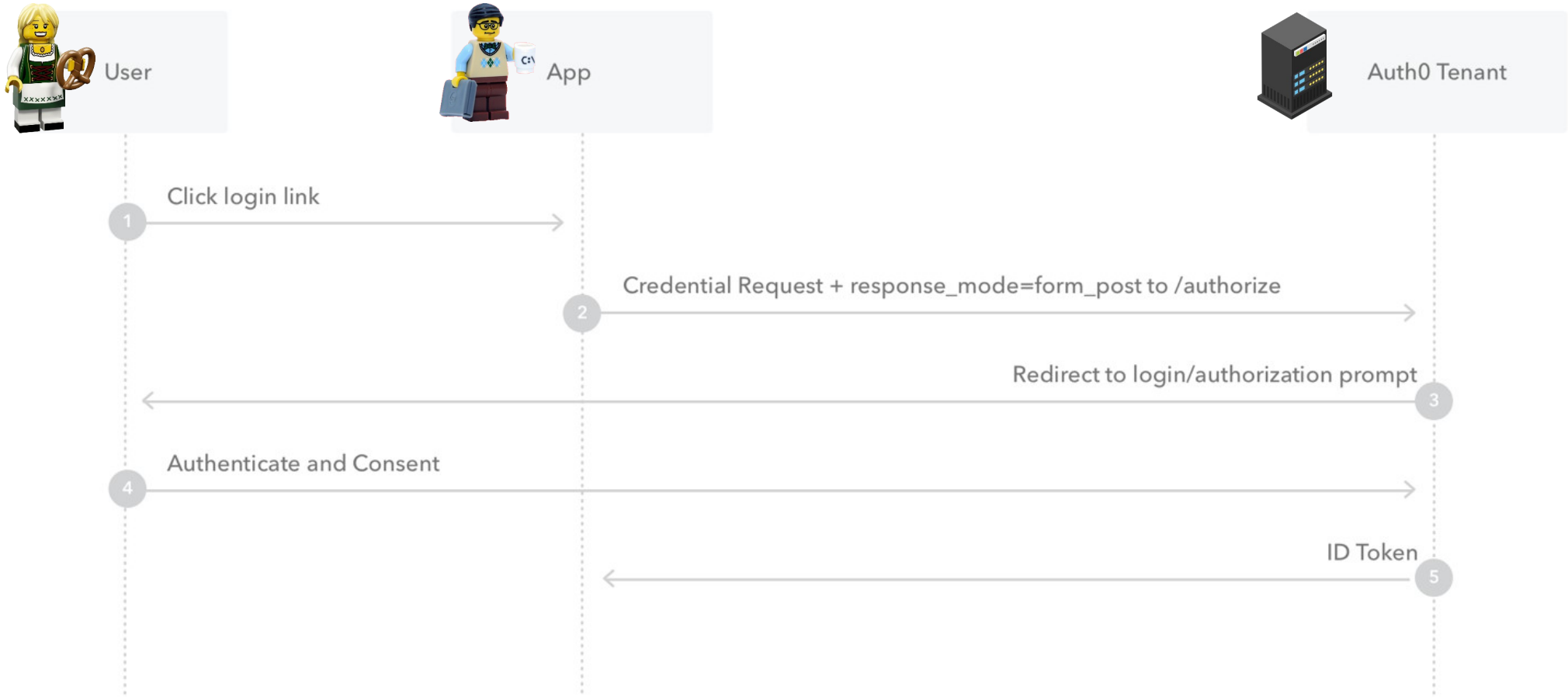
5 Request user data with Access Token

6 Response

Implicit Flow

- Nutzung nicht empfohlen
- Für client-seitige Apps
- Kein Refresh Token

Implicit


User
App
Auth0 Tenant
Click login link
1
Credential Request + response_mode=form_post to /authorize
2
Redirect to login/authorization prompt
3
Authenticate and Consent
4
ID Token
5

Quellen

- https://datatracker.ietf.org/doc/html/rfc6749
- https://datatracker.ietf.org/doc/html/rfc6750
- https://auth0.com/docs
- https://en.wikipedia.org/wiki/OAuth