

1. Erste Anfrage:
- 2.
3. GET <https://www.dlrg.net/oauth2/authorize>
- 4.
5. mit den Parametern:
- 6.
7. `response_type=code`
8. `client_id={vom AK IT erhaltene Client-ID}`
9. `redirect_uri={URL des eigenen Dienstes}`
10. `scope={eine Liste der Berechtigungen, die für den Dienst vom Nutzer erbeten werden}``properties`
11. `state={ein CSRF-Token}` (optional)
- 12.
13. Wenn der Benutzer sich einloggt und die Anfrage bestätigt erfolgt eine Weiterleitung auf die URL des eigenen Dienstes mit den Parametern
14. `code={der Autorisierungscode}`
15. `state={das CSRF-Token der vorherigen Anfrage}`
- 16.
- 17.
18. Nach dem Login und Bestätigung der Rechtegewährung muss der eigenen Dienst folgende Abfrage durchführen:
- 19.
20. POST <https://www.dlrg.net/oauth2/token>
- 21.
22. mit den Parametern:
- 23.
24. `grant_type=authorization_code`
25. `client_id={vom AK IT erhaltene Client-ID}`
26. `client_secret={vom AK IT erhaltenes Client-Passwort}`
27. `redirect_uri={URL des eigenen Dienstes}`
28. `code={der Autorisierungscode}`
- 29.
30. Es wird als Antwort ein JSON-Objekt gesendet mit folgenden Eigenschaften:
- 31.
32. `token_type: Bearer`
33. `expires_in: 3600`
34. `access_token: {das Token, welches u.a. die Benutzer-ID und die erhaltenen Rechte [Scopes] beinhaltet}`
35. `refresh_token: {ein "Auffrischungstoken", mit dem ein neues Token generiert werden kann, sollte dieses ungültig geworden sein}`
- 36.
37. Derzeit sind folgende Rechte vom Nutzer beantragbar:
38. `profile`: das Recht, den Benutzernamen, Vorname und Nachname des Nutzers abfragen zu dürfen
39. `email`: das Recht, die Email-Adresse des Nutzers abfragen zu dürfen
- 40.
- 41.
42. Diese Informationen sind abzufragen unter:
- 43.
44. GET <https://www.dlrg.net/oauth2/userinfo>
- 45.
46. mit dem `"Authorization"`-Header vom Typ `"Bearer"` und dem erhaltenen Token|