OpenID Connect und OAuth 2.0

Identity and Access Management (IAM) der DLRG

FAQ

Kann ich mich mit dem DLRG Account an meinen eigenen Diensten anmelden?

Durch den AK IT wird die Möglichkeit bereitgestellt sich mit dem DLRG Account per Single Sign-on (SSO) anzumelden. Hierzu werden die nachfolgenden Protokolle unterstützt.

- OAuth 2.0
- OpenID Connect (OIDC)

Nähere Informationen zu den beiden Protokollen können in einer Vielzahl im Internet gefunden werden. Unter anderem über OAuth oder OIDC. Im Normalfall bringt die verwendete Software für den Client auch eine eigene Dokumentation mit nützlichen Hinweisen und einer Anleitung zur Einrichtung mit.

Wo finde ich den Antrag für einen OIDC oder OAuth 2.0 Client?

Den Antrag findet ihr unten auf der Seite Hilfe & Support mit dem **IAM-Button**. Anschließend könnt ihr auswählen, ob ihr einen neuen Client beantragen oder einen bestehenden anpassen wollt.

Muss ich den Antrag nutzen?

Ja, der Antrag muss sowohl für neue Clients, als auch für die Änderung bestehender verwendet werden. Dadurch wird sichergestellt, dass ihr die notwendigen Berechtigungen in der jeweiligen Gliederung besitzt.

Welche Voraussetzungen muss ich für den Antrag erfüllen?

Für den Antrag über Hilfe & Support (IAM) müsst ihr

- Die Gliederung, zu welcher der Antrag zugeordnet werden soll, im ISC ausgewählt haben
- Mit eurem DLRG Account angemeldet sein, welcher das Recht **Internet-Webmaster** oder **IAM-Admin** in der Gliederung besitzt

Welche Informationen brauche ich für den Antrag?

Im Antrag über Hilfe & Support (IAM) müssen die nachfolgenden Informationen vorhanden sein.

- EDV-Nummer der Gliederung
- Name des Clients
- Beschreibung des Clients
- Art des Clients
  - Native (z.B. Mobile und Desktop Apps)
  - Single Page Web Applications (z.B. mit Angular, React, Vue)
  - Regular Web Applications (z.B. Node.js, Java, PHP)
- Root URL (Grundlegende URL des Dienstes z.B. *https://client.de*)
- Redirect/Callback URL (Callback zur Auswertung der Token z.B. *https://client.de/callback.php*. TLS muss verwendet werden.)

Diese Informationen werden im entsprechenden Support Formular abgefragt.

Welche Informationen erhalte ich nach erfolgreicher Prüfung des Antrags?

Nach erfolgreicher Prüfung des Antrages erhaltet ihr die nachfolgenden Informationen per Mail.

- Client ID für den OpenID Connect / OAuth 2.0 Client
- Client Secret / Verwendung von PKCE in Abhängigkeit von der Art des Clients.

Für die Konfiguration des Clients kann die nachfolgenden URLs in Abhängigkeit vom verwendeten Client genutzt werden.

- Provider/Issuer: https://iam.dlrg.net/auth/realms/master
- Discovery URL: https://iam.dlrg.net/auth/realms/master/.well-known/openid-configuration
- Authorization Endpoint: https://iam.dlrg.net/auth/realms/master/protocol/openid-connect/auth
- Token Endpoint: https://iam.dlrg.net/auth/realms/master/protocol/openid-connect/token

Ich habe Probleme meinen Client zu konfigurieren

Es erfolgt kein Support durch den AK IT bei der Einrichtung eines OAuth/OIDC Clients bei eigenen Anwendungen. Hilfestellungen sind der jeweiligen Dokumentation der verwendeten Software oder allgemein bezogen auf OAuth 2.0 und OIDC zu entnehmen.

Kann ich den DLRG Account mit meiner Synology Cloud nutzen?

Synology unterstützt aktuell (Dezember 2021) kein Login über OAuth 2.0 oder OIDC. Es gibt lediglich den OAuth Service, welcher jedoch ein eigener OAuth Server ist und kein Client.

Welche Scopes können verwendet werden?

Es stehen standardmäßig die Scopes *profile* und *email* zur Verfügung. Zusätzlich kann der Scope *openid* zur Nutzung des OIDC-Protokolls verwendet werden.

In Bearbeitung

Der Login mit dem DLRG Account an externen Diensten wurde überarbeitet. Diese Dokumentation ist dadurch stellenweise veraltet und wird aktuell überarbeitet.

Was ist oAuth2 (open Authorization) und wofür wird es verwendet?

- oAuth2 ist ein Protokoll, welches dem Nutzer ermöglicht, mehrere (externe) Dienste, die einer Anmeldung bedürfen, mit nur einem DLRG-Account zu nutzen. Das kann z. B. interessant sein, wenn eine Gliederung eine eigene Cloud (nicht die DLRG-Cloud) betreibt und möchte, dass sich die Mitglieder der Gliederung über den DLRG-Account anmelden können. So müssen sich die Mitglieder nicht mehrere Zugangsdaten merken.
    - ein gutes Beispiel für oAuth ist z.B. die Möglichkeit, sich mit seinem Facebook-Account bei Spotify anzumelden. Hier kommt ebenfalls oAuth zum Einsatz
- Das Anmeldeverfahren mit oAuth2 ist besonders sicher, da u. a. der externe Dienst nicht in den Besitz von Account-Passwörter gelangt und der Nutzer eine Kontrolle darüber hat, welche seiner Daten er für die Weitergabe freigibt.

Wie funktioniert oAuth2?

Die Funktion von oAuth2 erklären wir am Beispiel einer Gliederung, OG Musterstadt, die eine eigene Cloud betreibt.

Der Webmaster der OG Musterstadt hat auf seinem Cloud-Server den oAuth2-Client mit der beantragten Client-ID und dem Client-Passwort eingerichtet, so dass sich Mitglieder mit ihrem DLRG-Account in der Cloud der OG Musterstadt anmelden können.

Die Mitglieder rufen die Internetseite der Cloud auf, beispielhaft https://cloud.dlrg-musterstadt.de, und klicken dort als Anmeldemöglichkeit auf „mit DLRG-Account anmelden“.
Nun werden sie automatisch auf die Anmeldeseite des offiziellen DLRG-Servers geleitet auf dem der oAuth2-Server läuft. Über die im für die Weiterleitung zuständigen Link enthaltenen Daten (kryptische Zahlen- und Buchstabenfolgen) wird dem oAuth2-Server mitgeteilt, dass sich jemand mit seinem DLRG-Account in der Cloud der OG-Musterstadt anmelden möchte, welche Rechte die Cloud sich geben lassen möchte und auf welche Internetseite der Benutzer nach erfolgter Anmeldung zurückgeleitet werden soll.
Nach erfolgter Eingabe des Anmeldenamens und -passworts wird dem Mitglied in einer weiteren Abfrage aufgezeigt, welche Daten die Cloud übermittelt bekommen möchte. In diesem Fall den Benutzernamen, Vor- und Zunamen sowie die E-Mail-Adresse. Dies muss das Mitglied bestätigen und wird auf die Seite der Cloud zurück geleitet, auf der es nun angemeldet ist.

Das passiert für den Anwender nicht sichtbar im Hintergrund

Nachdem das Mitglied erlaubt hat, dass die geforderten Daten dem Drittanbieter, hier die Cloud der OG Musterstadt, preisgegeben werden dürfen, sendet der oAuth2-Server der DLRG eine Code an den oAuth2-Client auf dem Cloud-Server der OG Musterstadt.
Der oAuth2-Client der Cloud sendet nun eine erneute Abfrage an den oAuth-Server mit diesem Code, der spezifischen Client-ID sowie dem Client-Passwort um sich zu legitimieren. Diese Daten werden dabei nicht wie die der ersten Abfrage über den Browser, sondern im Hintergrund über eine gesicherte Verbindung übermittelt und ist für Angreifer nicht abfangbar und somit sicher vor Fremdzugriffen.
Nach erfolgter Legitimierung generiert der o2Auth-Server einen sogenannten Token, der ähnlich einem Cookie Informationen enthält und nur für einen bestimmten Zeitraum (in unserem Fall 1 Stunde) gültig ist.
Dieser Token wird an den oAuth2-Client der Cloud zurückgesendet, welcher diesen kurz verarbeitet und als letzten Legitimationsnachweis erneut an den oAuth2-Server zurücksendet.
Der oAuth2-Server weiß nun endgültig, dass die Cloud sie selbst ist und die Daten des Mitgliedes erhalten darf und erlaubt dem oAuth2-Client der Cloud den Zugriff auf die geforderten Daten (Benutzername, Vor- und Zuname und E-Mail-Adresse).

Vereinfacht erklärt

Vereinfacht gesprochen geht der oAuth2-Client der Cloud (im Weiteren Antragsteller genannt) zum oAuth2-Server der DLRG (im Weiteren Amt A und Amt B genannt) und stellt den Antrag auf Herausgabe von persönlichen Daten eines Mitmenschen.
Das Amt A prüft nun, ob der Antragsteller auch der ist, der er zu sein vorgibt und ob er einen berechtigten Anspruch auf die geforderten Daten hat sowie, ob die betroffene Person der Herausgabe der Daten eingewilligt hat.
Ist diese Prüfung positiv, stellt Amt A dem Antragsteller einen Erlaubnisschein (Token) aus, mit dem er zu Amt B gehen kann, welches die persönlichen Daten verwaltet.
Anhand des Erlaubnisscheins weiß das Amt B, dass der Antragsteller berechtigt ist, die gewünschten Daten zu erhalten und erteilt dem Antragsteller letztlich eine Auskunft.

Das Benutzerpasswort wurde bei dem gesamten Vorgang lediglich einmal bei der Anmeldung auf dem DLRG-Server eingegeben und nicht bei dem Drittanbieter. So hat der Drittanbieter keine Möglichkeit über seine Datenbank oder andere Wege das Benutzerpasswort des DLRG-Accounts auszulesen und dieses böswillig zu nutzen.

Fazit

Dem Endanwender macht oAuth2 das Leben deutlich einfacher, da man sich nicht mehr diverse Anmeldenamen und -passwörter für alle möglichen Dienste merken muss.
Einem potenziellen Angreifer wird es durch das Hin- und Herschicken von kryptischen Zeichen und das ständige Rückversichern (ähnlich Asterix und Obelix beim römischen Amt) sehr schwer bis quasi unmöglich gemacht die Anmeldedaten des Benutzers/Mitgliedes abzufangen und böswillig zu nutzen.