Vertrauenswürdige Clients

Theresa Henze - 2025-09-25 - Verschiedenes

Öffentliche Clients – Einsatz und Sicherheitsaspekte

Eine Bare.ID Applikation kann als öffentlicher OAuth2/OIDC Clients angelegt werden. **Öffentliche Client** Applikationen **können Anmeldedaten nicht sicher speichern**, z. B. browserbasierte Applikationen (SPAs) oder mobile Apps. Diese Clients **verwenden kein Client-Secret**, da die Speicherung im Frontend unsicher ist.

Wann öffentliche Clients verwendet werden sollten

- Für **Browser-Apps** (z. B. React, Angular)
- Für **mobile Apps** ohne sicheren Backend-Zugriff
- Wenn **kein Backend** vorhanden ist, um ein Secret zu schützen

Einschränkungen öffentlicher Clients

- Können sich nicht gegenüber Keycloak authentifizieren
- Anfällig für Token-Diebstahl, wenn nicht richtig konfiguriert
- Nicht geeignet für hochsensible Operationen ohne zusätzliche Sicherheitsmaßnahmen

Sicherheitsempfehlungen für öffentliche Clients

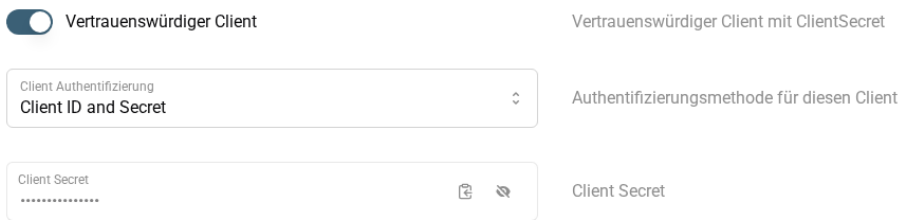
Zur Absicherung von öffentlichen Clients sollten folgende Maßnahmen umgesetzt werden:

- **PKCE verwenden (Proof Key for Code Exchange)**
  - Obligatorisch für SPAs und mobile Apps
  - Schützt vor Abfangen des Authorization Codes
- **CORS und Weiterleitungs-URIs strikt konfigurieren**
  - Nur bekannte, vertrauenswürdige URIs zulassen
  - Wildcards vermeiden
    - Wenn Wildcards in URLs aus technischen Gründen verwendet werden müssen, stelle sicher, dass die Domain- und Pfadpräfixe so streng wie möglich sind. Beachte, dass

Wildcards in der OAuth 2.1-Norm vollständig weggelassen werden und daher wann immer möglich vermieden werden sollten.

- **Content Security Policy (CSP) aktivieren**
  - Schutz vor XSS-Angriffen im Frontend
- **Lebensdauer von Tokens begrenzen**
  - Kurze Gültigkeit reduziert Risiko bei Token-Leakage
  - Refresh Tokens mit Bedacht verwenden
- **Kritische Operationen im Backend ausführen**
  - Sicherheitskritische Logik in Backend-APIs verlagern
  - Öffentliche Clients sollen keine sensiblen Daten direkt verarbeiten
- **Reduzieren der Token-Informationen**
  - Minimieren der im Token enthaltenen Daten, um das Risiko bei einem möglichen Token-Diebstahl zu verringern

Hinweis: Weitere Informationen zur Absicherung von Applikationen unter: https://datatracker.ietf.org/doc/html/rfc9700

Öffentlichen Client konfigurieren

- Lege die OAuth2/OIDC Applikation wie in der Seite [Applikation verbinden](https://support.bare.id/guides/bareid-handbuch/applikation-verbinden) beschrieben an.
- Deaktiviere den Schalter "Vertrauenswürdiger Client" im Abschnitt für "Einstellungen".