OIDC (OpenID Connect)

Inhaltsverzeichnis

OpenID Connect (OIDC) ist eine Identitätsschicht auf OAuth 2.0. Damit können sich Benutzer einmal zentral anmelden und Anwendungen erhalten geprüfte Identitätsinformationen per Token.

1 Funktionsweise

Ein Identity Provider authentifiziert den Benutzer und stellt ID- sowie Access-Tokens aus. Anwendungen (Relying Parties) vertrauen diesen Tokens statt eigener Passwortspeicher.

- **Authorization Code Flow:** üblicher, sicherer Web-Flow
- **ID Token:** Wer ist angemeldet?
- **Access Token:** Zugriff auf APIs/Ressourcen

2 Typische Einsatzbereiche

- Single Sign-On für Webapps und Portale
- Login bei Cloud- und Self-Hosted-Diensten
- Zentrale MFA-Durchsetzung über den IdP

3 Wichtige Hinweise

- Redirect-URIs und Client-Secrets müssen streng verwaltet werden.
- Token-Lebensdauer, Refresh und Logout-Strategien mitplanen.
- OIDC ist nicht dasselbe wie reines OAuth 2.0 ohne Identity-Schicht.

4 Fazit

OIDC ist der moderne Standard für SSO und föderierte Anmeldung – weniger Passwort-Wildwuchs, mehr zentrale Kontrolle über Identität und Sicherheit.