Übersicht gängiger OIDC-Flows

Flow	Beschreibung	Vorteile	Einsatzbeispiel	Besonderheiten
Authorization Code Flow	Client erhält Autorisierungscode und tauscht ihn gegen ID- und Access-Token ein.	Hohe Sicherheit, Tokens werden nicht im Browser ausgetauscht.	Serverseitige Web-Applikationen, Unternehmensportale.	Empfohlen für Web-Apps mit Backend, unterstützt PKCE.
Implicit Flow	Tokens werden direkt im Browser bei der Umleitung zurückgegeben, ohne Code-Zwischenschritt.	Schnell und einfach.	Single Page Applications (SPAs) ohne Backend	Weniger sicher, veraltet, heute oft durch Authorization Code Flow mit PKCE ersetzt.
Hybrid Flow	Kombination aus Authorization Code und Implicit Flow. Client erhält Code und Tokens gleichzeitig.	Flexibel, sofortiger Zugriff auf Nutzerinfo und Backend-Sicherheit.	Web-Applikationen, die schnelle und sichere Auth benötigen.	Komplexer, aber vielseitig.
Client Credentials Flow	Maschinen-zu-Maschinen-Authentifizierung ohne Nutzer, Access-Token für API-Zugriff.	Einfach und sicher für serverseitige Kommunikation.	Backend-Services, Microservices.	Kein Nutzerkontext.
Resource Owner Password Credentials Flow	Nutzer gibt Zugangsdaten direkt an den Client, der diese an den IdP weiterleitet.	Einfach, aber unsicher.	Selten empfohlen, nur in Ausnahmefällen.	Hohe Sicherheitsrisiken, nicht mehr empfohlen.