***OpenID Connect***

* Erlaubt einem Client (Service, Anwendung) die Identität eines Users zu bestätigen
  + Authentifizierung wird durch Authentifizierungsserver (OpenID Provider) ausgeführt
* Weiterhin können auch Basis-Informationen über den Benutzer und die authentifizierte Session abgefragt werden
* Auf Grundlage von OAuth 2.0

Authentifizierungsanfrage

Benutzer

Zustimmung

Client

benutzt OpenID Connect

Weiterleitung und Authentifizierung

Relying Party (RP)

Access Token

ID Token

OpenID Provider

implementiert OpenID Connect

* Informationen über den Benutzer werden in IDToken gespeichert (werden als JSON Web Token verschlüsselt an den Client geschickt)
* Zusätzlich wird im ID Token der legitime Empfänger des Tokens gespeichert (Audience Restriction)
* Schutz vor Hijacking (Kontrollübernahme eines Servers, Kontos oder Browser durch einen unautorisierten Dritten) und Substitutionsangriffen (Übernahme der Identität)
* Weitere Informationen zum Benutzer (eigene Musik, Bilder, Emails etc.) werden auf dem Server des OpenID Providers (OP) gespeichert
* Wenn sich ein Benutzer beim Client einloggen möchte, wird er direkt zum OP weitergeletet
* Authentifizierungsmethode wird durch den OP festgelegt
* Vorteil: kann abwechselnde und starke Authentifizierungsmethoden verwenden, ohne dass Client informiert oder geändert werden muss

Gültigkeitsdauer des Tokens ist von der Sicherheitsstufe des Authentifizierungsverfahrens abhängig

* Das ID Token wird nicht direkt zwischen OP und Client ausgetauscht, sondern über den Browser des Benutzers
* digitale Signatur gegen Modifikation nötig
* Schutz gegen Replay-Angriffe (Aufzeichnen von Daten und erneutes Senden der Daten

-> Vortäuschen einer fremden Identität) durch Anhängen eines Nonce (kryptografisch sichere Zufallszahl)