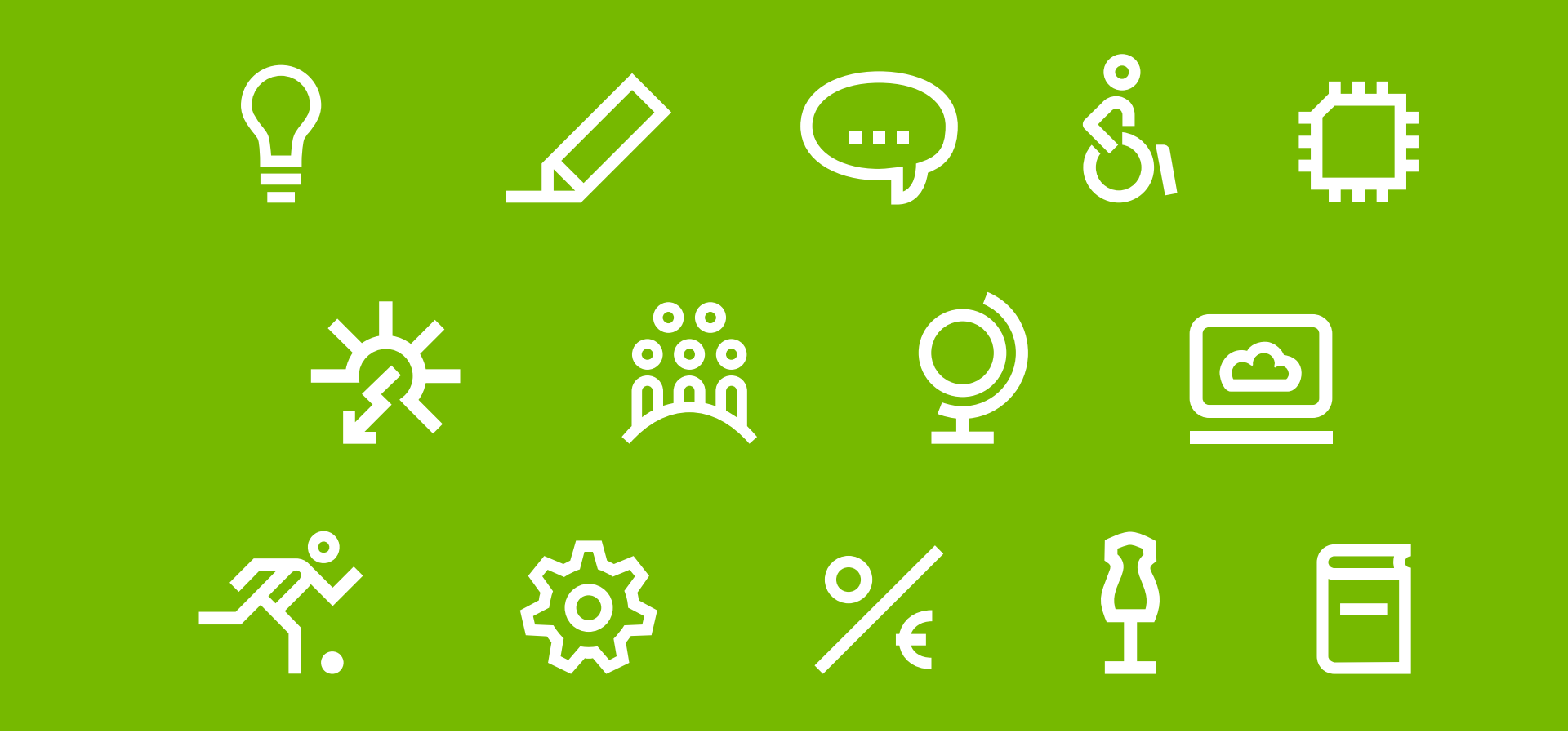


Hochschule für Technik und Wirtschaft Berlin

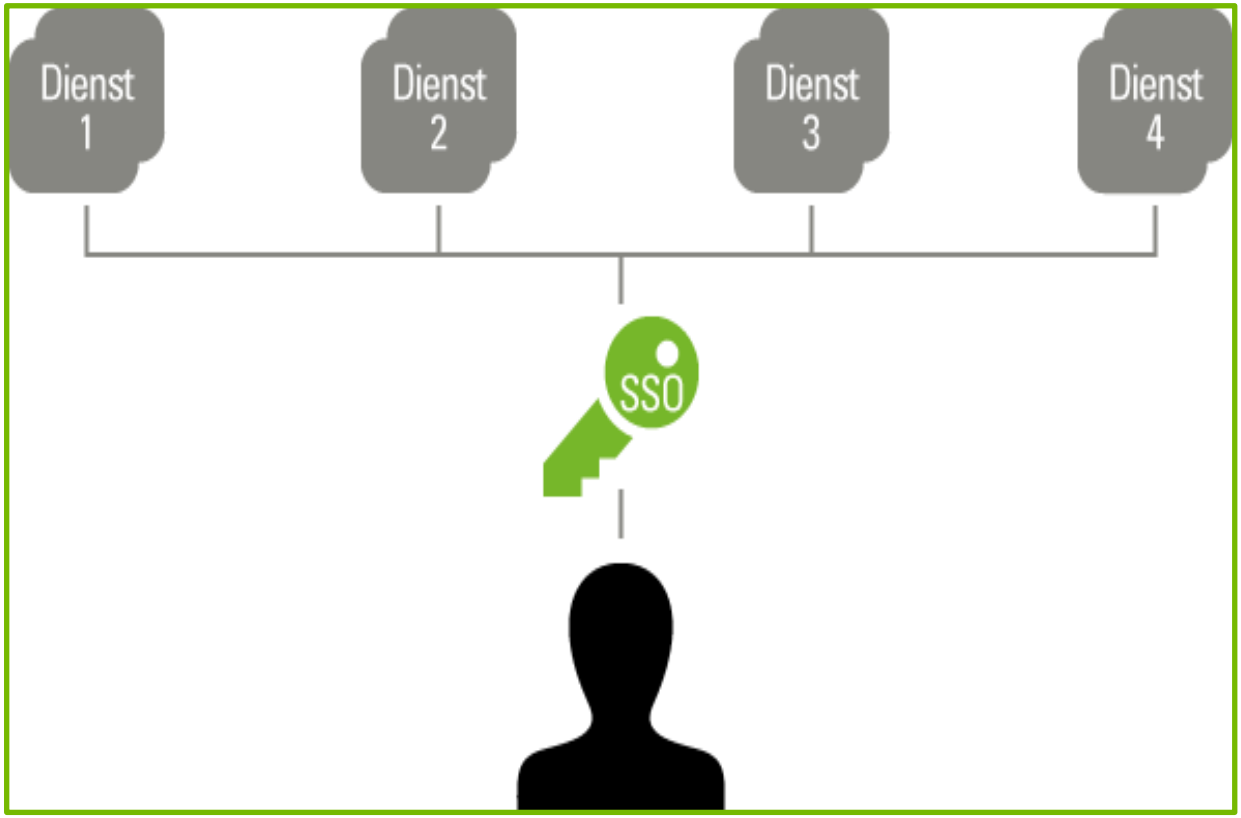
University of Applied Sciences

09.03.2021

Open ID Connect

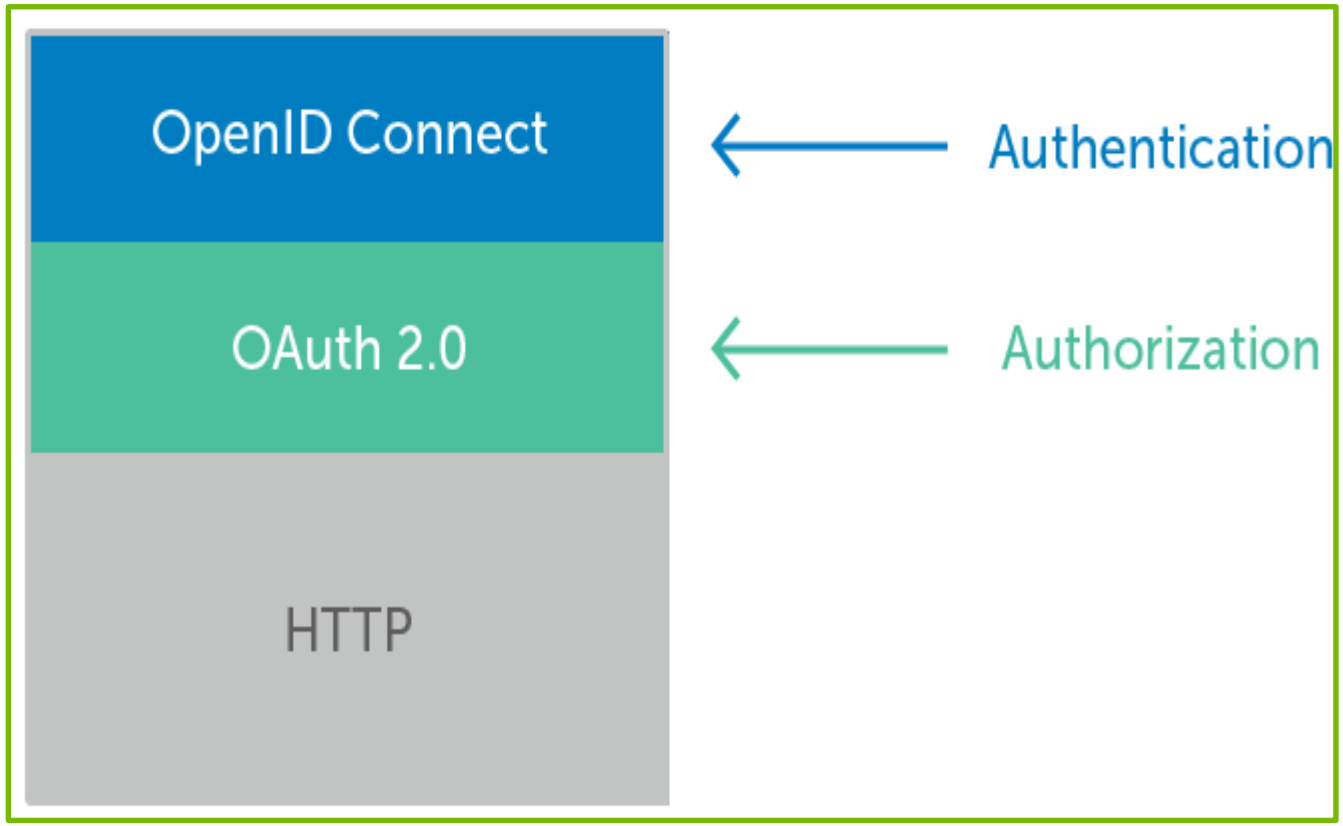
Quang Anh Nguyen, 566136

Single SignOn



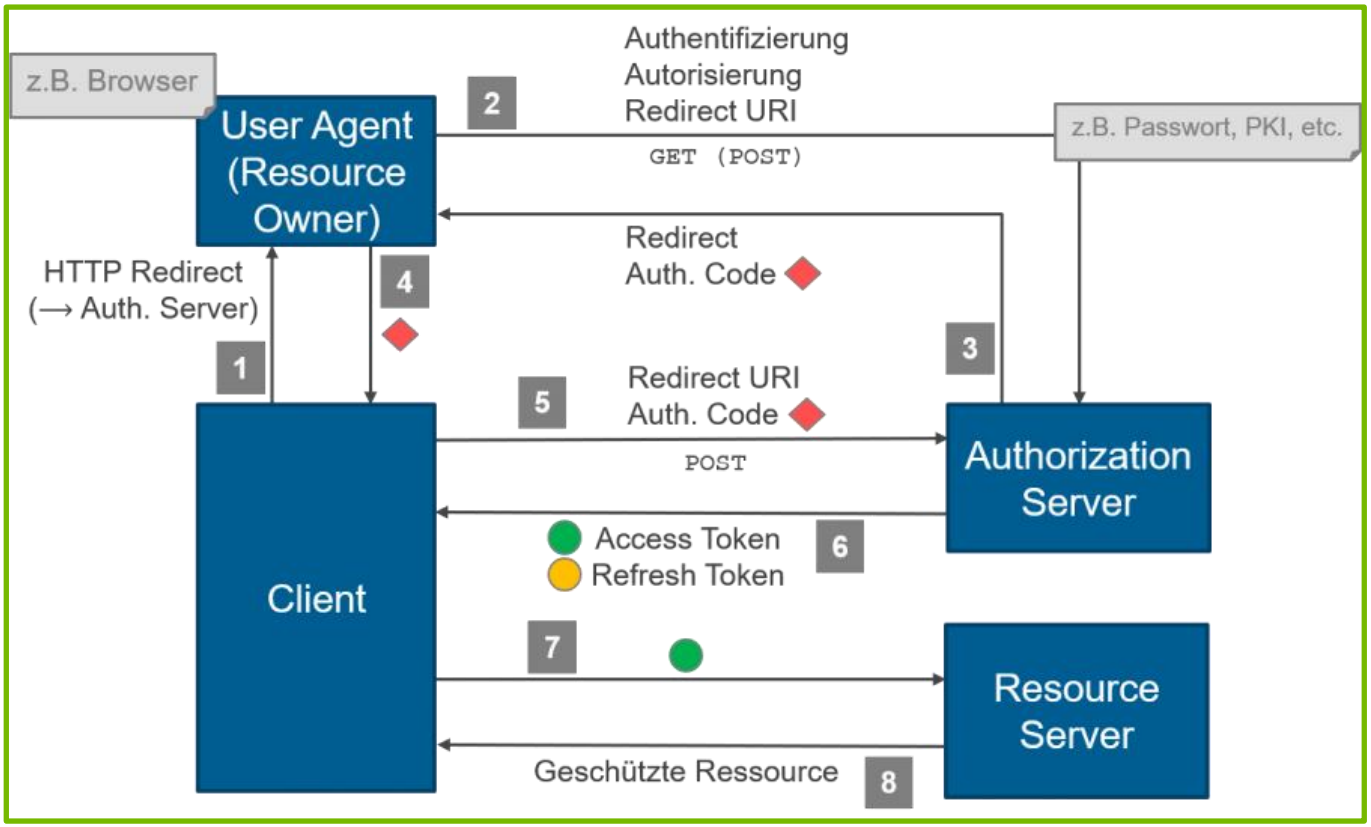
Single Sign-On (SSO): Authentifizierungsschema, das es einem Benutzer ermöglicht, sich mit einer einzigen ID und einem einzigen Passwort bei einem beliebigen von mehreren verwandten, aber unabhängigen Softwaresystemen anzumelden.

Definition



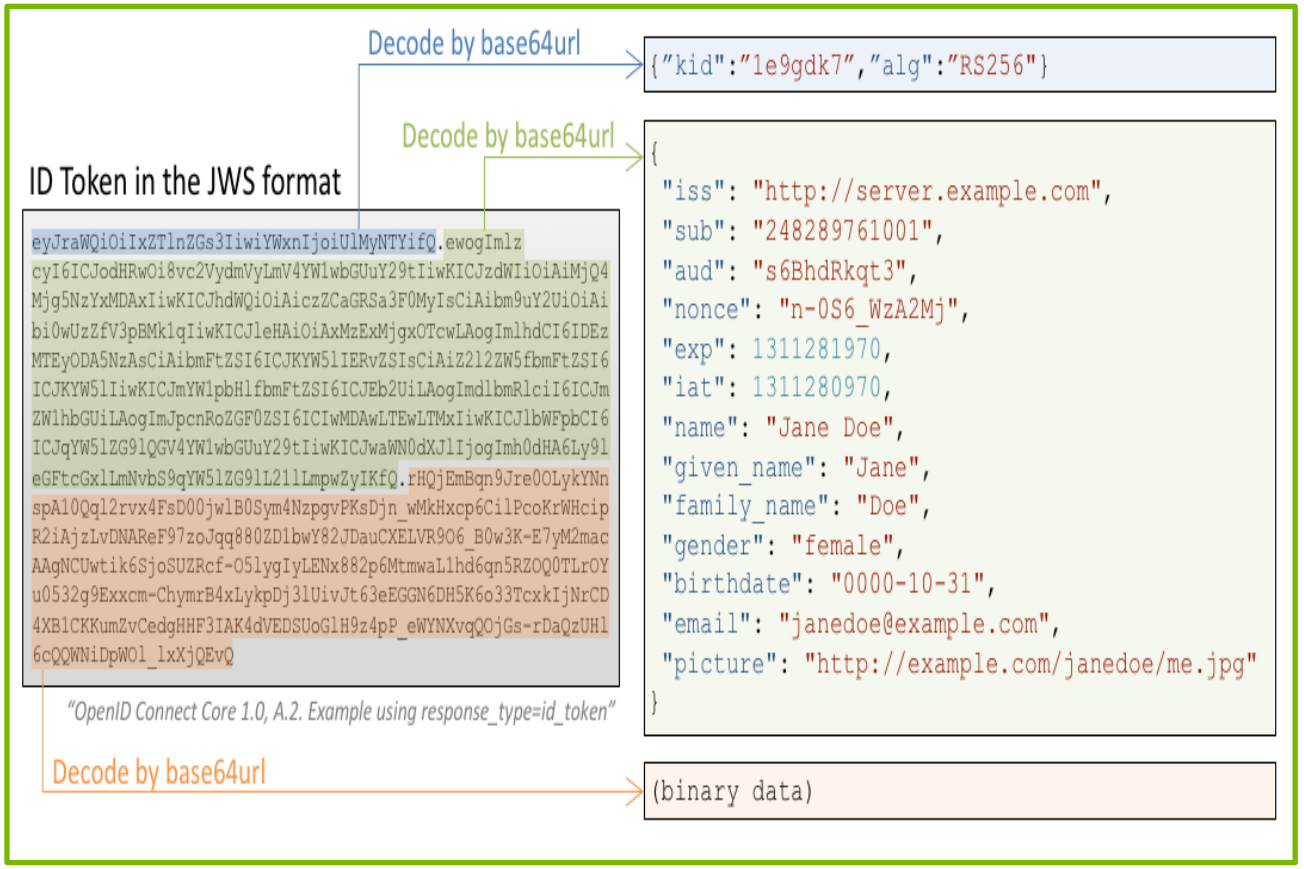
- OpenID Connect: eine einfache Identitätsschicht, die auf dem OAuth 2.0-Protokoll aufbaut.
- OAuth 2.0: ein Protokoll zur Autorisierung für Web-, Desktop und Mobile Anwendungen.

Authorization Code Flow



- Authorization Server(Autorisierungsserver): Token ausstellen
- Ressource Owner: die Berechtigung zum Zugriff auf den Ressourcenserver mit einem Zugriffstoken erteilt.
- Client : Die Anwendung, die das Zugriffstoken anfordert und es dann an den Ressourcenserver weitergibt.
- Ressource Server(Resourcenserver): Token überprüfen.

ID Token



ID Token: ein Standard-JWT-Format, signiert vom OpenID-Provider, enthalten Informationen über den Eigentümer der Ressourcen

Vor- und Nachteile

Vorteile

- Einfach zu konsumierende Identitäts-Tokens
- Basiert auf dem OAuth 2.0-Protokoll
- Einfachheit

Nachteile

- Identity Provider abhängig: wenn Prozess ausfällt, geht der Zugriff auf alle zugehörigen Systeme verloren
- Identity Provider verfolgen die Gewohnheit des Benutzers.


Vielen Dank
für Ihre
Aufmerksamkeit!

Quelle

https://openid.net/connect/

https://www.oose.de/blogpost/oauth-openid-connect-und-jwt-wie-haengt-das-alles-zusammen-teil-1/

https://www.okta.com/openid-connect/

https://darutk.medium.com/understanding-id-token-5f83f50fa02e

https://www.security-insider.de/was-ist-single-sign-on-sso-a-631479/

www.htw-berlin.de