Didaktische Reduktion für Sek1 am Beispiel des Anwendungsfalles *Instagram mit Facebook Login*

Alice und Bob benutzen Instagram zum Ablegen von Fotos und Videos. Dabei haben Alice und Bob in ihren Instagram Einstellungen die Option 'Privates Konto' gewählt, so dass nur bestätigte Abonnenten die Fotos und Videos sehen können.
Damit Alice und Bob sich für Instagram kein weiteres Passwort merken müssen, wählen sie die Variante 'Mit Facebook anmelden' und es laufen die folgenden Schritte** ab:
1) mit der Wahl von 'Mit Facebook anmelden' erfolgt die Weiterleitung zum Facebook Login
2) beim Facebook Login wird ergänzend zu den Facebook Zugangsdaten (Benutzername/Passwort) auch die Zustimmung des Zugriffs von Instagram auf das Facebook Konto eingeholt
3) nach der erfolgten Zustimmung sendet Facebook einen Code zurück
4) Instagram tauscht diesen Code bei Facebook gegen ein Access Token aus
5) mit dem Access Token kann Instagram die Ressourcen des angemeldeten Benutzers (z.B. Alice oder Bob) freischalten

Zu beachten: Beim gesamten Ablauf gelangen die vom Benutzer im Facebook Login Dialog eingegebene Zugangsdaten (Benutzernamen und Passwort) nie zu Instagram und zu den geschützten Ressourcen. Damit wird die Handhabung der Logins vereinfacht (Single-Sign-On). Wie die Grafik rechts unten zeigt, existieren neben dem 'Facebook Login' zahlreiche andere Social Logins mit Google, Twitter, Github etc.

Im eIdLab.ch Labor kann der oben beschriebene Login Prozess mit den Codes und den Access-Tokens interaktiv erforscht werden.
Im Arbeitsblattentwurf des Kapitels A1 aus dem Abschnitt Arbeitsblätter/Werkzeuge sind Anregungen zum Erforschen des oben beschriebenen Login Prozesses aufgeführt. Dabei werden die folgenden Themenbereiche angesprochen:
- erforschen des ‘rezeptartigen’ Ablaufs (Algorithmus / Login Flow) von Social Logins
- aufzeigen, dass die Social Logins auf den Standards OAuth 2.0 und OpenID Connect basieren
- die Risiken von Social Logins erforschen und greifbar machen und die Einwände gegen die Verwendung von Social Logins als Bildungsidentität diskutieren
- aufzeigen, dass die Standards der Social Logins auch für Bildungsidentitäten geeignet sind und diskutieren, in welchen Schulen, Gemeinden und Kantonen bereits solche Bildungsidentitäten im produktiven Einsatz sind
- sicher Passwörter, Passwörter codieren (Hashing, Salt)

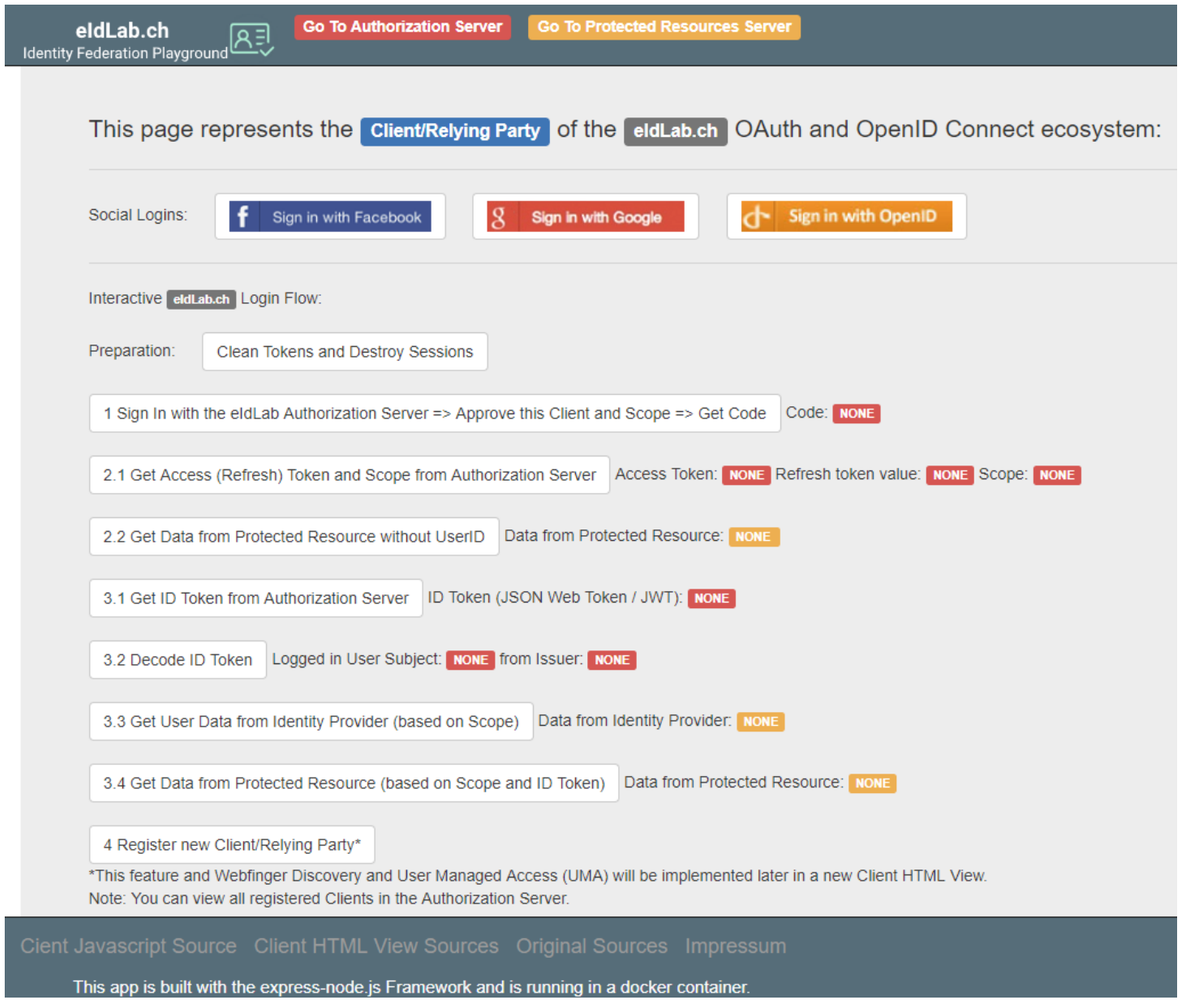
**Die oben aufgeführten Loginschritte sind gegenüber der Realität vereinfacht. Im Kapitel F5.3 Didaktische Reduktion für die Maturitätsschulen erfolgt eine komplexere Beschreibung mit zusätzlichen Hinweisen zu den Sicherheits-mechanismen. Im Arbeitsblattentwurf für die Berufsbildung werden die technischen Hintergründe zum ‘Login with Email’ erläutert. Dazu dienen dienen die OpenID Connect Standarderweiterungen Discovery und Dynamic Client Registration.

CH Open Education Day 6. April 2019 / PHBern, vonRoll-Areal / Raum B 204 / Claude Jacob, buerojacob.ch

Single Sign-on mit Facebook, Google etc.: Was passiert im Hintergrund?

Bei der domänenübergreifenden Anmeldung im Web werden Informationen zwischen dem aufgerufenen Webdienst (Serviceprovider SP) und dem für die Anmeldung benutzten Identitätsanbieter (Identity Provider IdP) ausgetauscht. Dabei werden die Anmeldeinformationen in der Regel mit elektronischen Schlüsseln, sogenannten Tokens, übermittelt. Im Workshop werden die Struktur, der Inhalt und der Fluss von openAuthorization und openID Tokens mit Entwicklertools und dem Identity Federation Playground 'eIdLab.ch' visualisiert, analysiert und die Transparenz von 'open source' erlebbar gemacht. Die konzept- und handlungsorientierten Workshopexperimente sind auf den Lehrplan21 (...Aufbau und Funktionsweise von informationsverarbeitenden Systemen verstehen...) und den neuen gymnasialen Rahmenlehrplan (...abstrakte Prinzipien und Prozesse thematisieren und greifbar machen...) ausgerichtet.

Dokumentation: eIdLab.ch



Screenshot https://www.innoedu.ch:9000/

Didaktische Reduktion für Maturitätsschulen am Beispiel des Anwendungsfalles *Übetrittsprozess Sek1/Sek2*

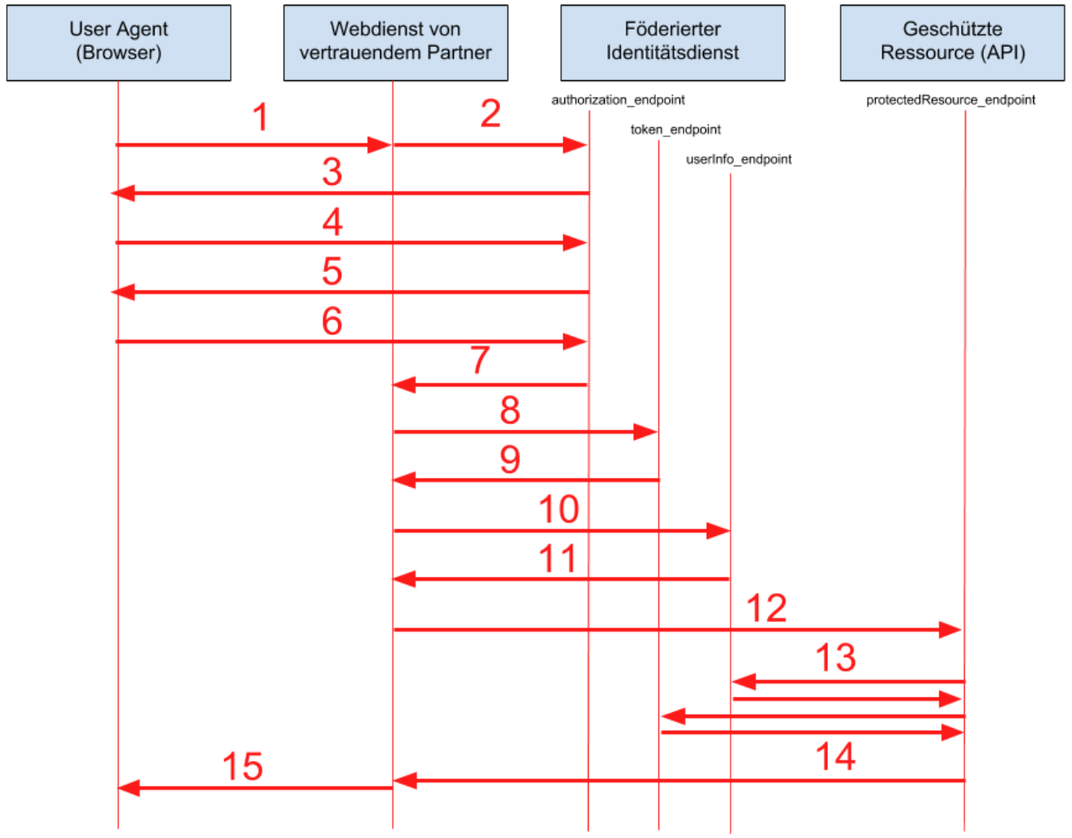
Lernende greifen im Rahmen des Übertrittsverfahrens beispielsweise auf die folgenden Webdienste der vertrauenden Partner-Webdienste zu (siehe Grafik rechts unten):
- Prim/Sek1: Informations- und Prüfungsvorbereitungsunterlagen, Portfolio mit eigenen Prüfungsdokumenten ...
- Kantonsverwaltung: Prüfungsanmeldeunterlagen ...
- Berufsmaturitätsschule: Prüfungsaufgebot, Prüfungsplan, Prüfungsresultate ....

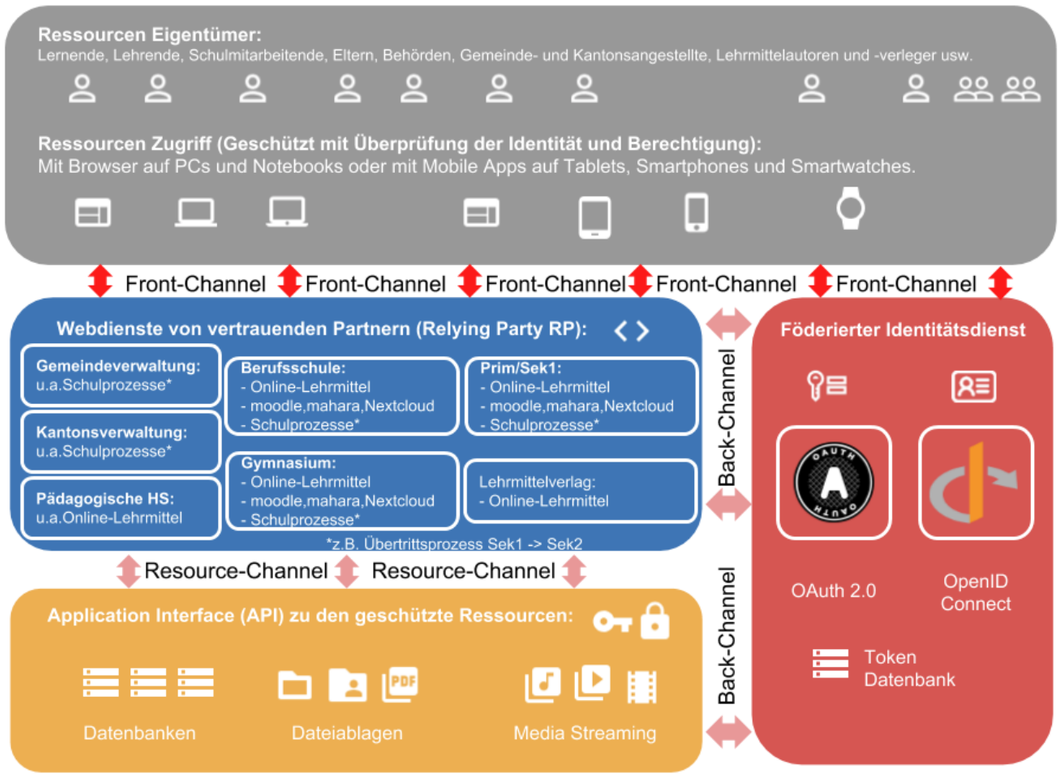
Diese Zugriffe laufen immer nach dem gleichen Standard ab (siehe Grafik rechts):
1) User Zugriff auf den Webdienst vom vertrauenden Partner (z.B. Berufsschule)
2) Klick auf Anmeldung und Umleitung an den föderierten Identitätsdienst (z.B. Kantonale BildungsID)
3) Loginformular im Browser anzeigen
4) Eingabe der Zugangsdaten im Loginformular durch den User
5) Zustimmungsformular im Browser anzeigen, auf welchen Ressourcenbereich der Webdienst zugriffsberechtigt ist
6) der User gewährt Zugriff auf den angezeigten Bereich
7) der Identitätsdienst sendet einen Code an den Webdienst
8) der Webdienst sendet den Code zurück und verlangt ein Access Token
9) der Identitätsdienst sendet das Access Token an den Webdienst
10) der Webdienst verlangt mit dem Access Token die User Informationen
11) der Identitätsdienst sendet die User Informationen an den Webdienst
12) der Webdienst sendet das Access Token und die User Informationen an das API (Application Interface) der Geschützten Ressourcen
13) das API der Geschützten Ressource überprüft (validiert) das Access Token und die User Informationen
14) das API der Geschützten Ressource sendet die Geschützten Ressourcen an den Webdienst
15) der Webdienst sendet die Geschützten Ressourcen an den Browser des Users

Zu beachten: Beim gesamten Ablauf gelangen die vom Benutzer eingegebene Zugangsdaten (z.B. Benutzernamen und Passwort) nie zum aufgerufenen Webdienst und zu den geschützten Ressourcen. D.h. für alle in diesem Verbund beteiligten Partner Webdienste bleiben die Zugangsdaten verborgen. Damit wird die Sicherheit erhöht. Gleichzeitig wird für die Benutzer die Handhabung der Logins vereinfacht, da für alle beteiligten Webdienste für den betreffenden Benutzer immer die gleichen Zugangsdaten gelten (Single-Sign-On).

Im eIdLab.ch Labor kann der oben beschriebene Login Prozess mit den Codes, den Access-Tokens, den OpenID User Informationen und den Geschützten Ressourcenzugriffen interaktiv erforscht werden.

Der oben beschriebene Vorgang ist gegenüber der Realität vereinfacht dargestellt. Hier finden Sie detailliertere Informationen zu OAuth 2.0 und OpenID Connect:
https://connect2id.com/learn/oauth-2
https://connect2id.com/learn/openid-connect





A.1 Arbeitsblattentwurf Sek 1, Maturitätsschulen, Berufsbildung (Diskussionspapier)

A1.1 Anwendungsbeispiele (Kap F1) diskutieren
- Erfahrungsaustausch in der Klasse (z.B. mit Kurzreferaten) zum bisherigen Umgang mit Social Logins und allfällig bisher benutzen Bildungsidentitäten

A1.2 im eIdLab.ch Labor die Social Logins ausführen
- was ist immer gleich -> herantasten an Standards -> Fortsetzung in A1.5

A1.3 Didaktische Reduktion OAuth 2.0 / OpenID Connect Login Flow für Sek1 (Kap F5)
-> Didaktisch reduzierten Login Flow greifbar machen -> Begriffsklärung zu den Tokens und User Infos bei den Social Logins im eIdLab.ch Labor

A1.4 Risiken von Social Logins / Access-Tokens entwenden und missbrauchen
- Diskussion 'Big Data': Social Login Anbieter können Daten sammeln, wann ihre user welche Apps benutzen
Weitere Infos dazu:
https://fides.educa.ch/de/id-praxis/darwin-daten-und-wir
https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news/facebook.html
https://www.channelpartner.de/a/wo-bleibt-der-siegeszug-von-social-login,3332670
https://brands-consulting.eu/facebook-connect-google-sign-in-und-co-welche-risiken-fuer-den-datenschutz-social-login-verursacht
https://www.heise.de/tipps-tricks/Facebook-Daten-schuetzen-durch-Deaktivieren-der-App-Integration-4000590.html
- Diskussion 'Unsicherer Umgang mit Identitätsdaten' (siehe beispielsweise https://www.heise.de/newsticker/meldung/Facebook-Hack-Sensible-Daten-von-Millionen-Nutzern-entwendet-4190206.html -> Access-Token entwendet)
- Experiment 'Access-Token weitergeben (entwenden)' -> Austausch der Access-Token via http://collabedit.com/
-> Fremde Identitätsdaten abrufen mit
Facebook Access-Token: https://graph.facebook.com/me?fields=id,name,email&access_token=
https://graph.facebook.com/me/permissions?&access_token=
Google Access-Token: https://openidconnect.googleapis.com/v1/userinfo?access_token=
OpenID Connect Access-Token: https://www.innoedu.ch:3010/oidc/me?access_token=
eIdLab.ch Access-Token: https://www.innoedu.ch:9002/userinfo?access_token=
Ermittlung des userinfo Endpoints:
Facebook: Facebook benutzt eine proprietäre OAuth 2.0 Authetifikationserweiterung -> keine .well-known/openid-configuration
Google: https://accounts.google.com/.well-known/openid-configuration
OpenId: https://www.innoedu.ch:3010/oidc/.well-known/openid-configuration

A1.5 Die Notwendigkeit von Offenen Standards greifbar machen
- Arbeitsblatt zu
https://www.etsi.org/images/files/Education/Understanding_ICT_Standardization_LoResPrint_20190125.pdf
erstellen
- weitere Links: https://fsfe.org/activities/os/os.de.html
https://www.isoc.de/wer-macht-das-internet/documents/Martin-Peter.pdf
https://open-stand.org/resources/infographics/
https://www.heise.de/newsticker/meldung/Fuenf-Grundsaetze-fuer-offene-Standards-1702793.html
https://www.itu.int/web/pp-18/uploads/itu-setting-the-standard-infographic.pdf
http://www.ech.ch/
http://www.sbbk.ch/dyn/23086.php

A1.6 Sichere Passwörter / Hashcodierung (Bsp: Lp21:DIeuv Lehrplan21:Digitale Identitäten einsetzen und verstehen)
https://www.passwortcheck.ch/passwortcheck/passwortcheck
https://www.hsg-kl.de/faecher/inf/krypto/hash/index.php
https://einfachinformatik.inf.ethz.ch/

A.2 Arbeitsblattentwurf Maturitätsschulen, Berufsbildung (Diskussionspapier)

A2.1 Experimente mit eIdLab.ch Labor OpenID Connect Login Flow

A2.2 Zuordnen des Login Flows aus A2.1 zur didaktischen Reduktion Sek 2 (Kap F5)
(siehe auch https://www.slideshare.net/briandavidcampbell/openid-connect-a-simplesic-single-signon-identity-layer-on-top-of-oauth-20)

A2.3 Experimente mit https://developers.google.com/oauthplayground/
Step 1 -> Scope openid
Step 2 -> Get Tokens
Step 3 -> z.B. userInfo wie in A1.4 abrufen

A2.4 Experimente mit https://oidcdebugger.com/
-> mit Response type experimentieren
-> JWT dekodieren -> https://jwt.io/
-> Authorize URI: https://www.innoedu.ch:3010/oidc/auth
Client Konfigurationen:

```
{client_id: 'token_id_token_code',
 client_secret: 'super_secret',
 grant_types: ['authorization_code', 'implicit'],
 response_types: ['token id_token code'],
 redirect_uris: ['https://oidcdebugger.com/debug'],
 token_endpoint_auth_method: 'none'}
```

Response type: x code x token x id_token
https://www.innoedu.ch:3010/oidc/auth?client_id=token_id_token_code&redirect_uri=https%3A%2F%2Foidcdebugger.com%2Fdebug&scope=openid&response_type=code%20token%20id_token&response_mode=form_post&state=1111&nonce=09z8lhea1j6b
-> Weitere Client Konfigurationen werden hier abgelegt.

A2.5 Signieren und Verschlüsseln von JWT's
https://www.cryptool.org/de/

A.3 Arbeitsblattentwurf Berufsbildung - Infrastrutur Projekte/Szenarien für Schulumgebungen umsetzen:

https://eidlab-identity-federation-playground.openses.org/pageselect?selectedLanguageId=de&selectedToolbarTabId=tab01&selectedWpPage=arbeitsblattentwurf-berufsbildung