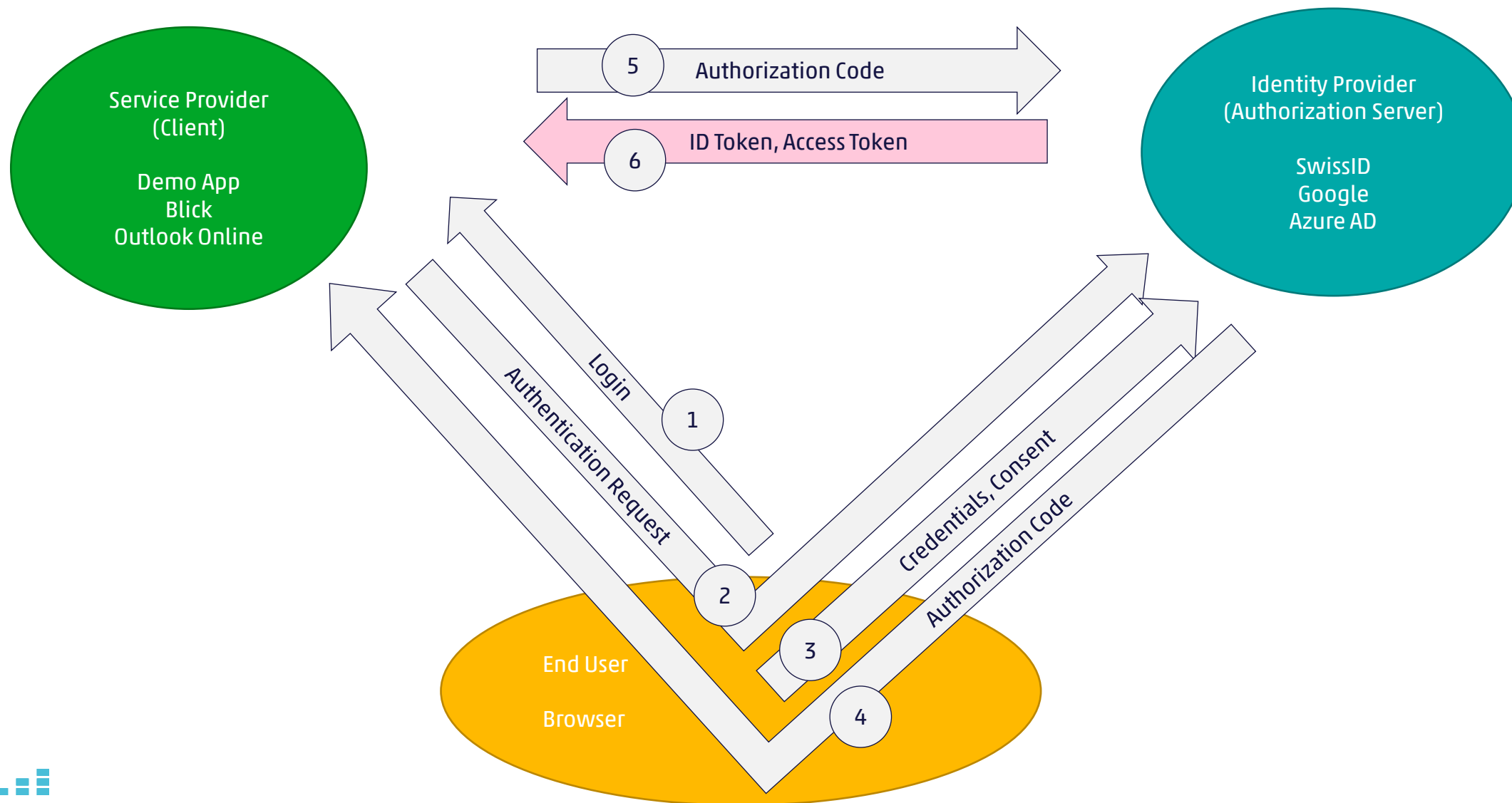


Herbsttagung 2021

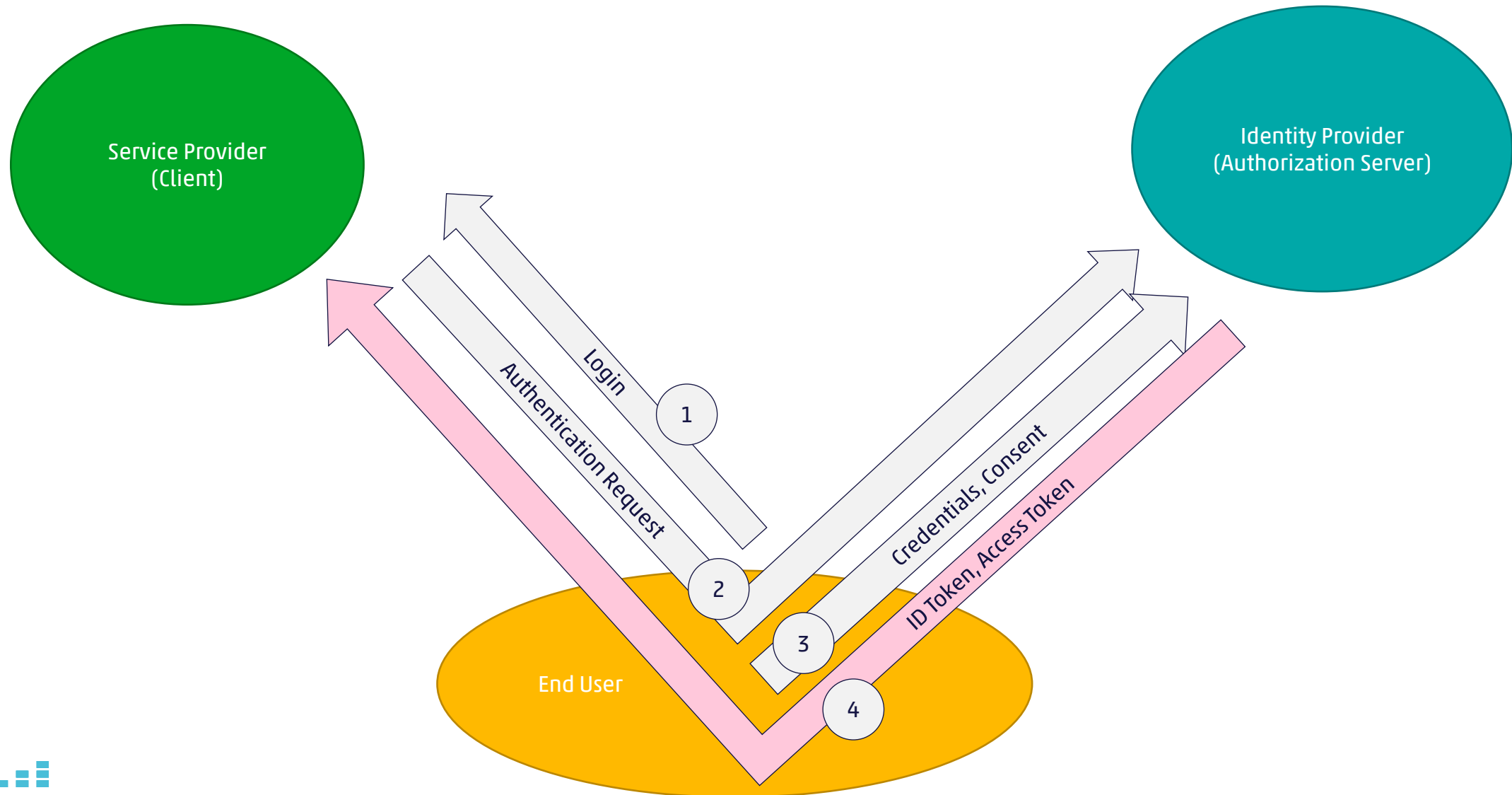
Demo: Föderation

Thomas Lüthi
Zürich, 8. September 2021

OpenID Connect – Authorization Code Flow



OpenID Connect – Implicit Code Flow



Demo: Login with OneLog (Ringier)

The screenshot shows a web browser window with the URL `welcome.onelog.ch/?client=iq6JnMWfrXwdLWQxNSPzICChFaMI2O9B&interaction=5nkzAR0FUpLAZ-vWfmHCB&I...`. The page header includes the **Blick** logo and the text "Login powered by OneLog".

[Zurück](#)

Einloggen oder registrieren

Wir sind Partner vom zentralen Schweizer Medien-Login OneLog.
[Mehr Infos](#)

E-Mail

Weiter Sie haben kein Konto? [Hier registrieren](#)

ODER

Mit SwissID fortfahren **Mit Facebook fortfahren**

Mit Google fortfahren **Mit Apple fortfahren**

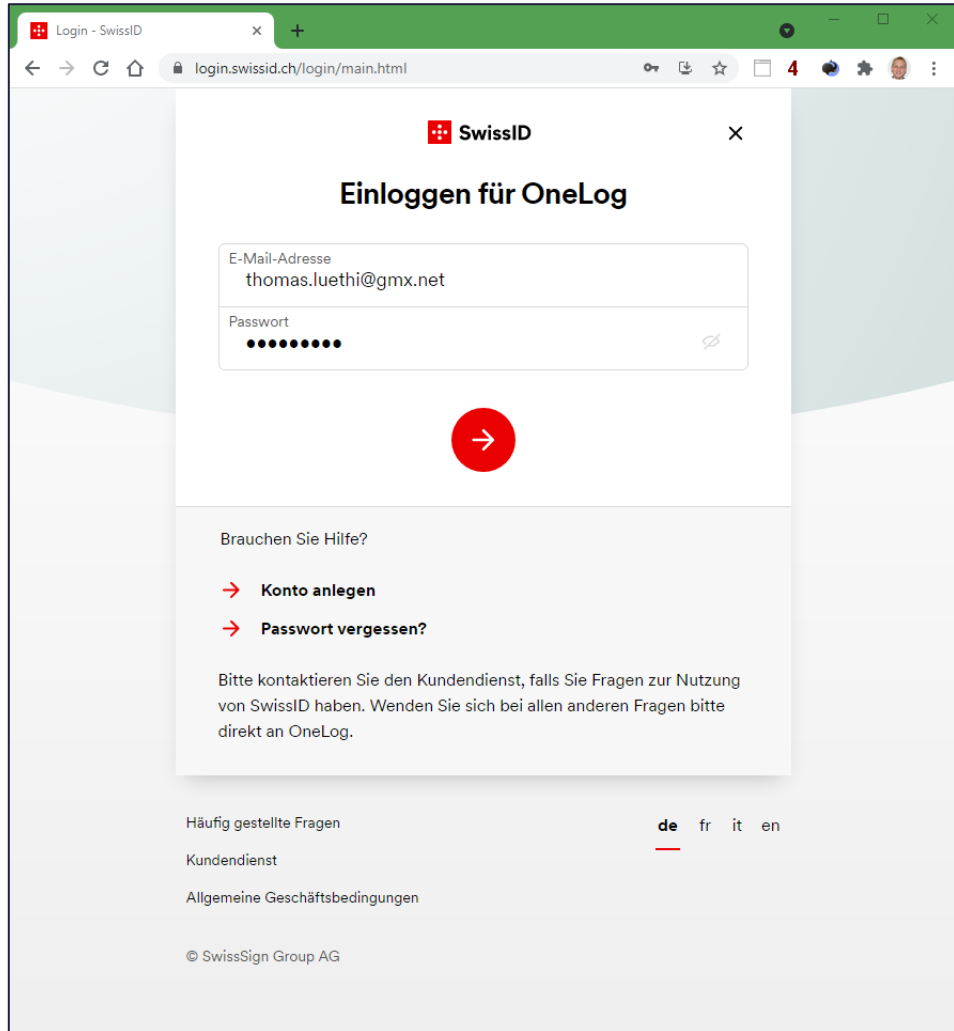
Einloggen und mitdiskutieren

- ✓ Werden Sie Teil der Blick-Community
- ✓ Mitdiskutieren über brisante Themen
- ✓ Nur ein Login für einen einfachen Zugang zu allen Online-Portalen mit OneLog

OneLog
Das Schweizer Medien-Login

[Weitere Portale und Infos](#)

Demo SwissID: Login / Consent



The image shows the SwissID login page for OneLog. It features a central white box with a red SwissID logo and the title 'Einloggen für OneLog'. Below the title are two input fields: 'E-Mail-Adresse' with the value 'thomas.luethi@gmx.net' and 'Passwort' with masked characters. A large red circular button with a white right-pointing arrow is positioned below the password field. To the left of the main box, there is a section titled 'Brauchen Sie Hilfe?' with two links: '→ Konto anlegen' and '→ Passwort vergessen?'. Below these links is a paragraph of text: 'Bitte kontaktieren Sie den Kundendienst, falls Sie Fragen zur Nutzung von SwissID haben. Wenden Sie sich bei allen anderen Fragen bitte direkt an OneLog.' At the bottom left, there are links for 'Häufig gestellte Fragen', 'Kundendienst', and 'Allgemeine Geschäftsbedingungen'. At the bottom right, there are language selection buttons for 'de', 'fr', 'it', and 'en', with 'de' currently selected. The footer includes the copyright notice '© SwissSign Group AG'.

SwissID

Einloggen für OneLog

E-Mail-Adresse
thomas.luethi@gmx.net

Passwort
●●●●●●●●

→

Brauchen Sie Hilfe?

→ **Konto anlegen**

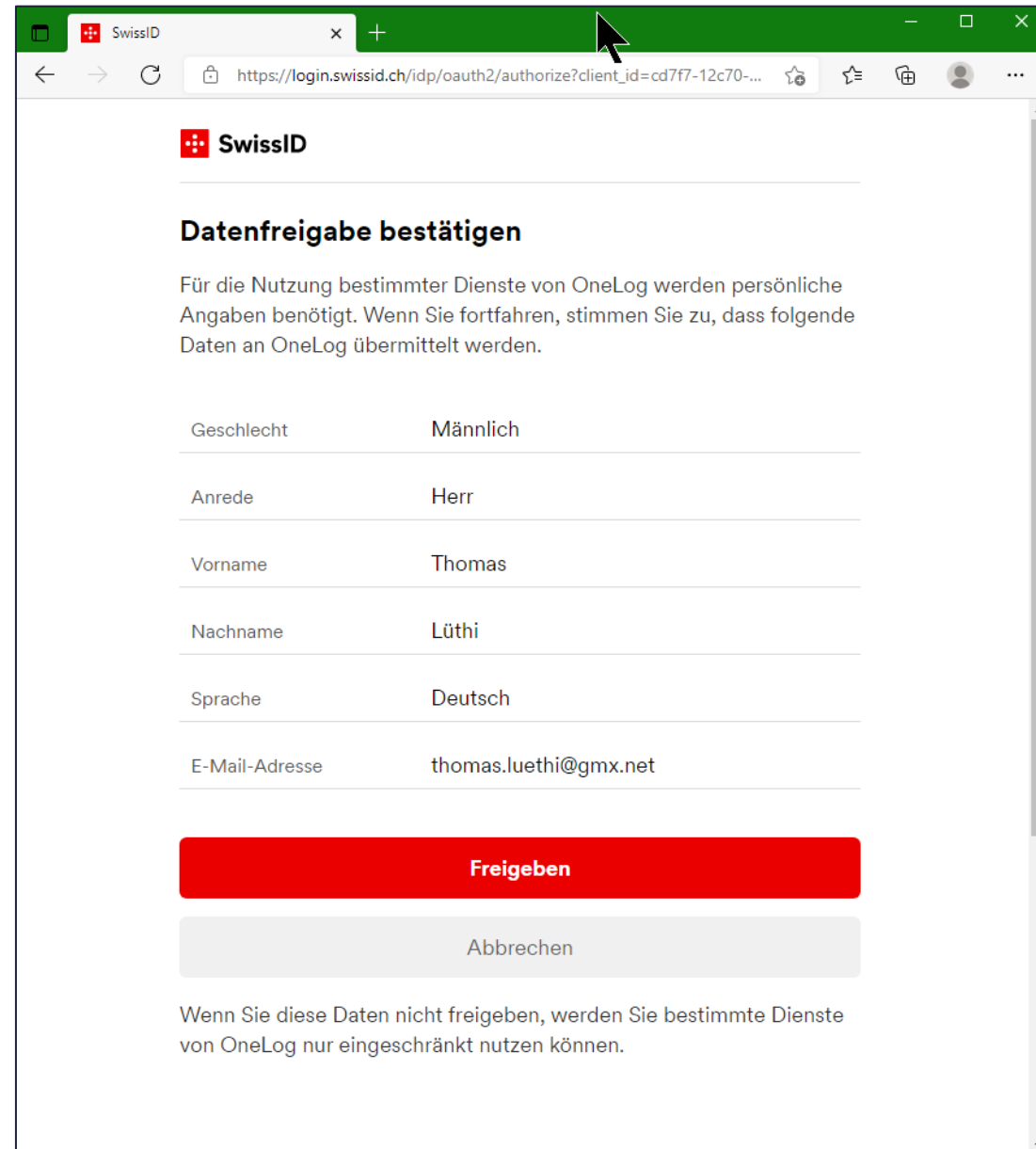
→ **Passwort vergessen?**

Bitte kontaktieren Sie den Kundendienst, falls Sie Fragen zur Nutzung von SwissID haben. Wenden Sie sich bei allen anderen Fragen bitte direkt an OneLog.

Häufig gestellte Fragen
Kundendienst
Allgemeine Geschäftsbedingungen

de fr it en

© SwissSign Group AG



The image shows the SwissID consent page for OneLog. It features a white box with a red SwissID logo and the title 'Datenfreigabe bestätigen'. Below the title is a paragraph of text: 'Für die Nutzung bestimmter Dienste von OneLog werden persönliche Angaben benötigt. Wenn Sie fortfahren, stimmen Sie zu, dass folgende Daten an OneLog übermittelt werden.' Below this text is a table with two columns: the first column lists the data types, and the second column lists the corresponding values. The table has six rows: 'Geschlecht' with 'Männlich', 'Anrede' with 'Herr', 'Vorname' with 'Thomas', 'Nachname' with 'Lüthi', 'Sprache' with 'Deutsch', and 'E-Mail-Adresse' with 'thomas.luethi@gmx.net'. Below the table are two buttons: a red button labeled 'Freigeben' and a grey button labeled 'Abbrechen'. At the bottom of the page, there is a paragraph of text: 'Wenn Sie diese Daten nicht freigeben, werden Sie bestimmte Dienste von OneLog nur eingeschränkt nutzen können.'

SwissID

Datenfreigabe bestätigen

Für die Nutzung bestimmter Dienste von OneLog werden persönliche Angaben benötigt. Wenn Sie fortfahren, stimmen Sie zu, dass folgende Daten an OneLog übermittelt werden.

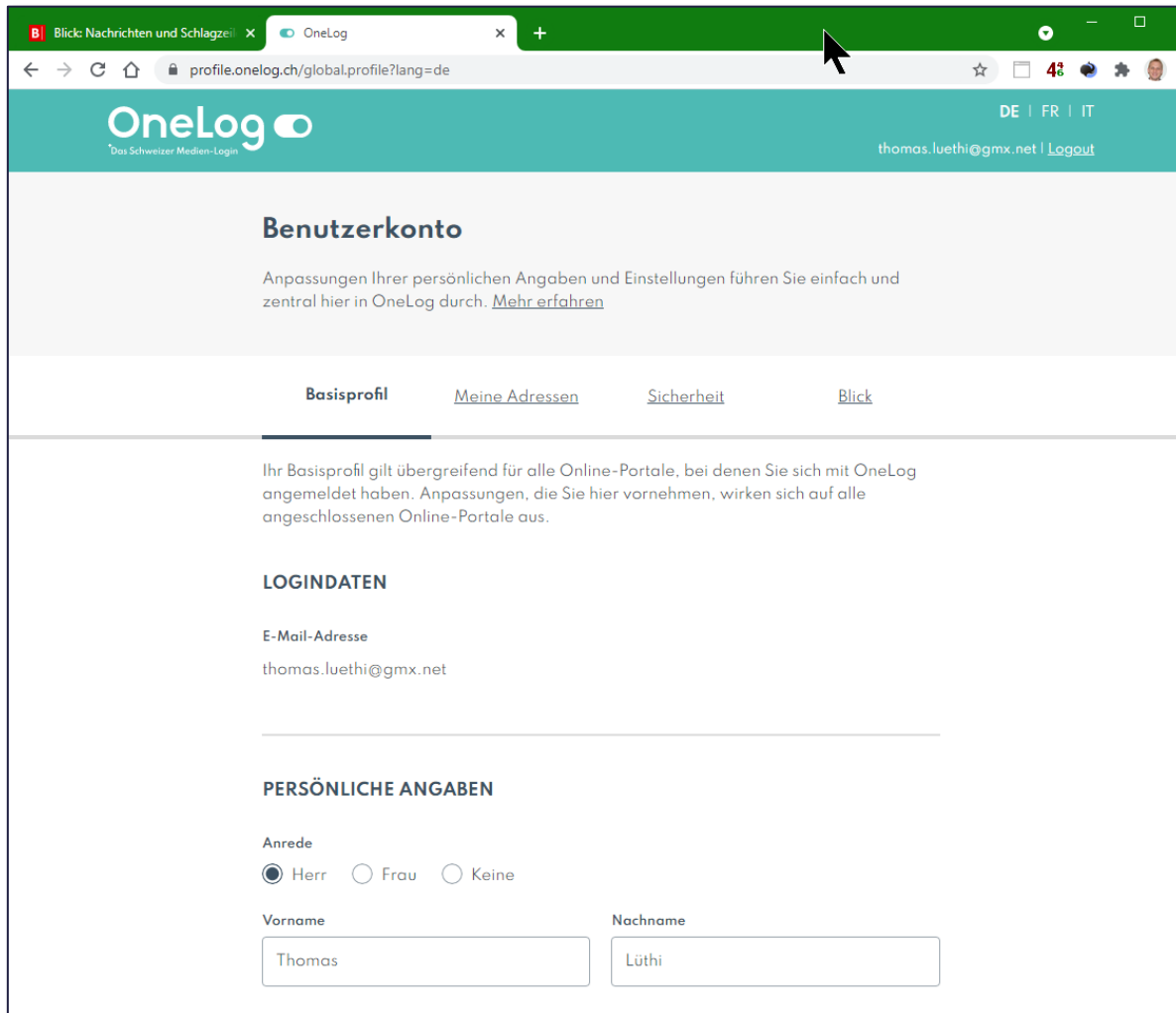
Geschlecht	Männlich
Anrede	Herr
Vorname	Thomas
Nachname	Lüthi
Sprache	Deutsch
E-Mail-Adresse	thomas.luethi@gmx.net

Freigeben

Abbrechen

Wenn Sie diese Daten nicht freigeben, werden Sie bestimmte Dienste von OneLog nur eingeschränkt nutzen können.

Demo SwissID: Account / Consent



The screenshot shows the OneLog user account page. The browser address bar displays 'profile.onelog.ch/global.profile?lang=de'. The page header includes the OneLog logo and the user's email 'thomas.luethi@gmx.net' with a 'Logout' link. The main section is titled 'Benutzerkonto' and contains a description of the account settings. Below this, there are four tabs: 'Basisprofil', 'Meine Adressen', 'Sicherheit', and 'Blick'. The 'Basisprofil' tab is active, showing the user's email address 'thomas.luethi@gmx.net' under the 'LOGINDATEN' section. The 'PERSÖNLICHE ANGABEN' section includes a gender selection (Herr, Frau, Keine) and input fields for 'Vorname' (Thomas) and 'Nachname' (Lüthi).

Benutzerkonto

Anpassungen Ihrer persönlichen Angaben und Einstellungen führen Sie einfach und zentral hier in OneLog durch. [Mehr erfahren](#)

Basisprofil [Meine Adressen](#) [Sicherheit](#) [Blick](#)

Ihr Basisprofil gilt übergreifend für alle Online-Portale, bei denen Sie sich mit OneLog angemeldet haben. Anpassungen, die Sie hier vornehmen, wirken sich auf alle angeschlossenen Online-Portale aus.

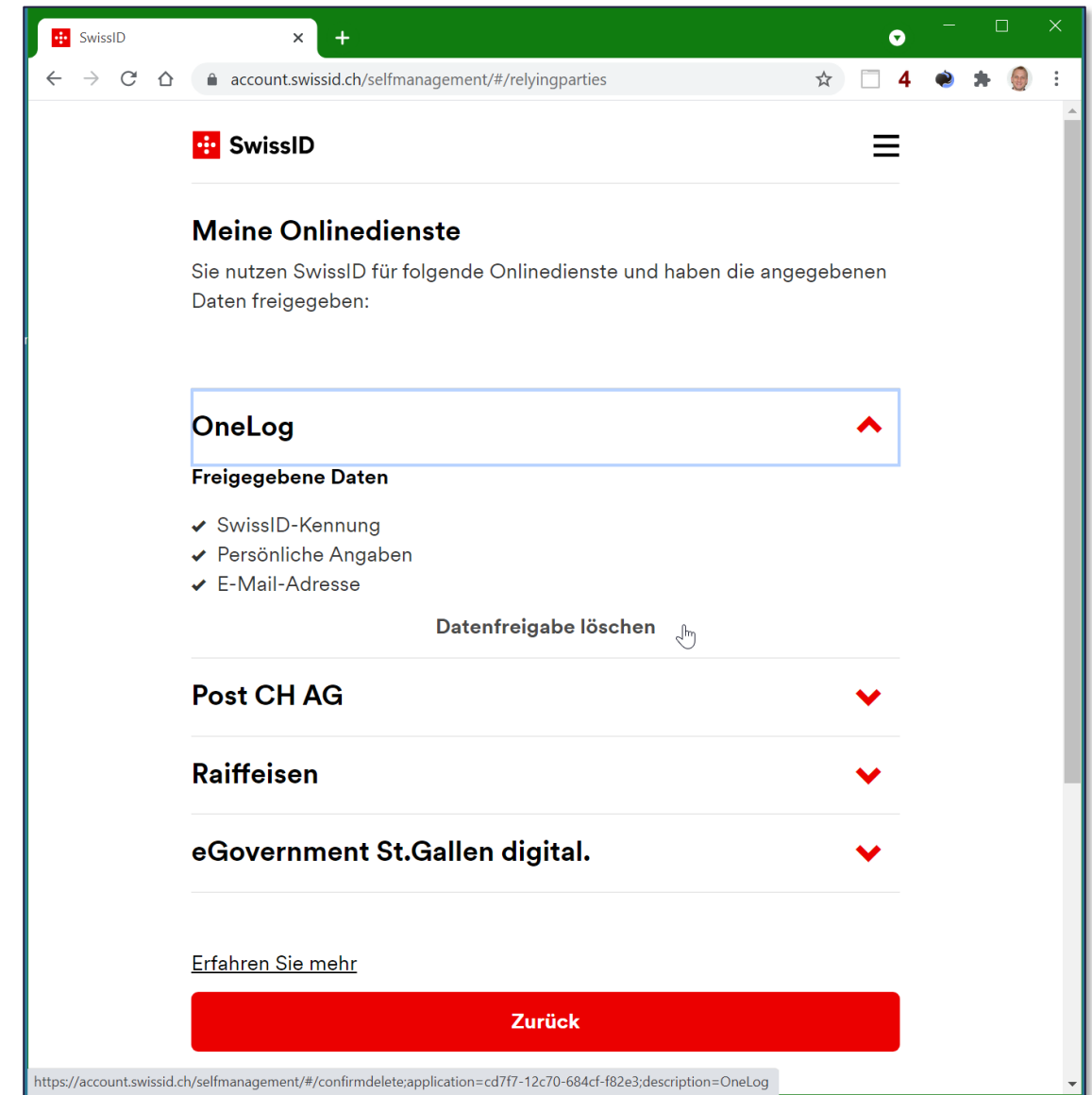
LOGINDATEN

E-Mail-Adresse
thomas.luethi@gmx.net

PERSÖNLICHE ANGABEN

Anrede
☒ Herr ☐ Frau ☐ Keine

Vorname Nachname
Thomas Lüthi



The screenshot shows the SwissID self-management page. The browser address bar displays 'account.swissid.ch/selfmanagement/#/relyingparties'. The page header includes the SwissID logo and a menu icon. The main section is titled 'Meine Onlinedienste' and contains a description of the services. Below this, there is a list of services: 'OneLog', 'Post CH AG', 'Raiffeisen', and 'eGovernment St.Gallen digital.'. Each service has a red checkmark icon. The 'OneLog' service is highlighted with a blue border. Below the list, there is a link 'Datenfreigabe löschen' and a red button 'Zurück'.

SwissID

Meine Onlinedienste

Sie nutzen SwissID für folgende Onlinedienste und haben die angegebenen Daten freigegeben:

OneLog 

Freigegebene Daten

- ✓ SwissID-Kennung
- ✓ Persönliche Angaben
- ✓ E-Mail-Adresse

[Datenfreigabe löschen](#) 

Post CH AG 

Raiffeisen 

eGovernment St.Gallen digital. 

[Erfahren Sie mehr](#)

Zurück

<https://account.swissid.ch/selfmanagement/#/confirmdelete;application=cd7f7-12c70-684cf-f82e3;description=OneLog>

Demo: OneLog Login Network Flow

Burp

Project

Intruder

Repeater

Window

Help

Burp Suite Professional v2021.6.2 - blick login.burp -

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Logger

Extender

Project options

User options

SAML Raider Certificates

SAML

Intercept

HTTP history

WebSockets history

Options

Filter: Showing only highlighted items

#	Host	Method	URL	Comment
2581	https://id.onelog.ch	GET	/federated/callback/swissid?code=MKzhINQJQKNTIU5hq1p4pHZUiko&iss=https%3A%2F%2Flogin.swissid.ch%3A443%2Fidp%2F...	Redirect to Service with Auth Code
2563	https://login.swissid.ch	GET	/login/?goto=https%3A%2F%2Flogin.swissid.ch%3A443%2Fidp%2Foauth2%2Fauthorize%3Fclient_id%3Dcd7f7-12c70-684cf-f82e...	Login
2562	https://login.swissid.ch	GET	/idp/oauth2/authorize?client_id=cd7f7-12c70-684cf-f82e3&scope=openid%20email%20profile&response_type=code&redirect_...	Send Auth Request
2561	https://id.onelog.ch	POST	/federated/begin	Start Login

Demo: Complete Login Flow with Demo App

Burp Suite Professional v2021.6.2 - blick login.burp - licensed to cnlab secur				
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options SAML Raider Certificates SAML OpenAPI Parser				
Intercept HTTP history WebSockets history Options				
Filter: Showing only highlighted items				
#	Host	Method	URL	Comment
2621	http://10.10.10.10:8000	GET	/public/app.css	Browser: Access App
2620	https://cnlab.eu.auth0.com	GET	/.well-known/jwks.json	App: Get Signing Keys
2619	https://cnlab.eu.auth0.com	POST	/oauth/token	App: Get ID Token
2618	http://10.10.10.10:8000	GET	?code=jcZWKSxXmj4eusyn&state=862ed2b5c7f008374775ec6e1f0c628c	Send Auth Code to App
2616	https://cnlab.eu.auth0.com	POST	/u/login?state=hKFo2SAxZ1RQVndMZzg0YThYNWIEZmd1dnpZeUZKY1FQQjZkVaFur3VuaXZlcnNhbc1sb2dpbqN0aWTZIGIDbmRk...	Login
2614	https://cnlab.eu.auth0.com	GET	/authorize?scope=openid%20profile%20email&response_mode=query&response_type=code&redirect_uri=http%3A%2F%2F10....	Send Authorization Request to Authorization Server
2613	http://10.10.10.10:8000	GET	/login.php	Start Login
2611	http://10.10.10.10:8000	GET	/	Get Loginpage

Demo: ID Token

Request

Pretty Raw Hex \n

```
1 POST /oauth/token HTTP/1.1
2 Content-Length: 236
3 User-Agent: GuzzleHttp/7
4 Host: cnlab.eu.auth0.com
5 Auth0-Client: eyJuYWllIjoiYXV0aDAtcGhwIiwidmVyc2lvbiI6IjcuOS4yIiwiaWZwZW52Ijpb7InBocCI6IjcuNC4zIn19
6 Content-Type: application/json
7 Connection: close
8
9 {
  "client_secret": "c73ZoKzW9jya4mr9x7hx9roMpbXFVIGblptKgi",
  "redirect_uri": "http://10.10.10.10:8000/",
  "code": "jc2WKSXmj4eusyn",
  "grant_type": "authorization_code",
  "client_id": "BhknrAmrvYiIPtNZ2aEr5fpTut8CI35B"
}
```

JWT

```
Headers := {
  .. "alg": "RS256",
  .. "typ": "JWT",
  .. "kid": "iBtJClnH-bvLCnNWJh2n"
}

Payload := {
  .. "nickname": "thomas.luethi",
  .. "name": "Thomas Lüthi",
  .. "picture": "https://s.gravatar.com/avatar/f849de8e6077d94a16032e225664af86?s\u003d480\u0026",
  .. "updated_at": "2021-09-01T08:13:15.838Z",
  .. "email": "thomas.luethi@cnlab.ch",
  .. "email_verified": true,
  .. "iss": "https://cnlab.eu.auth0.com/",
  .. "sub": "auth0|612ec51a4b1db80068fcbd54",
  .. "aud": "BhknrAmrvYiIPtNZ2aEr5fpTut8CI35B",
  .. "iat": 1630484001,
  .. "exp": 1630520001,
  .. "nonce": "6e02c1432cdc6db1955e5f4c8460429a"
}

Signature := "RkwyXjvidr736tH9F2TrjFT-diIht_HsuiPXw9ESc_-yBj6qM2m7d0Ke-wwXqbzn1SuuCBE3zvuBuzE9V"
```



Vielen Dank für Ihre
Aufmerksamkeit_

Thomas Lüthi
Thomas.Luethi@cnlab.ch

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland