TMF – Technologie- und Methodenplattform
für die vernetzte medizinische Forschung e.V.

Samply.Auth

MAGIC: IT-Werkzeuge für die medizinische Verbundforschung

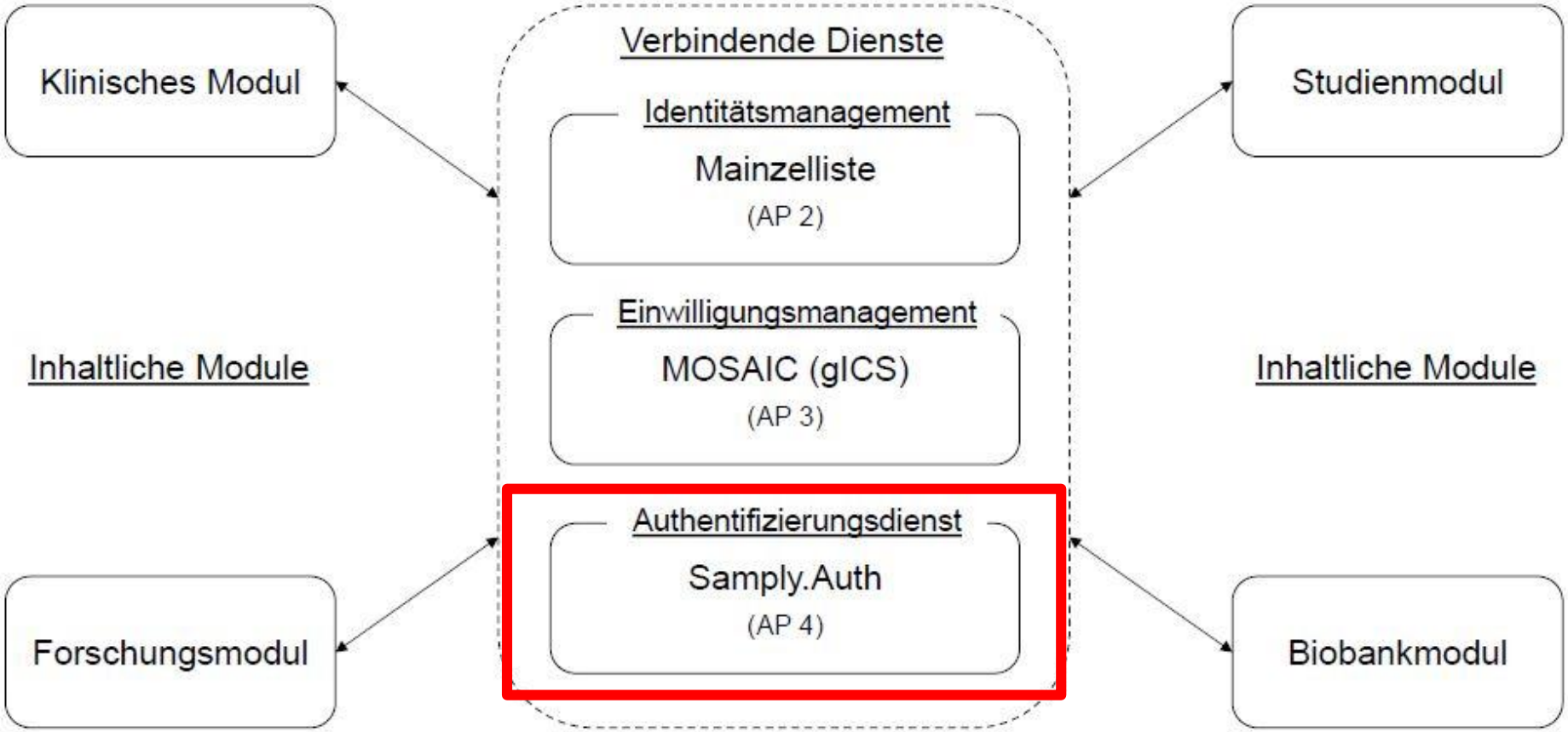
TMF Tutorials | Bonn | 19.03.2019

Galina Tremper

Deutsches Krebsforschungszentrum Heidelberg

Verbundinformationssysteme

Einordnung in den TMF-Leitfaden



Authentifizierung und Autorisierung

- **Authentifizierung** - Prüfung der vom Nutzer behaupteten Identität
  - Wer bin ich?

- **Autorisierung** - Zuteilung der Zugriffsberechtigungen des Users
  - Welche Berechtigungen habe ich?

☑ Dienst 1
☑ Dienst 2
☒ Dienst 3

Übersicht

1. Authentifizierungsdienst – Kernfunktionalität
2. Samply.Auth: Installation und Konfiguration
3. Anbindung an Samply.Auth - Beispiel-Ablauf
4. Föderierte Authentifizierung
5. Demo

Authentifizierungsdienst

- Verwaltung von Benutzern und Berechtigungen
- Zentralisierte Verwaltung der Nutzerberechtigungen von Webanwendungen
- Verwaltung von Benutzern und Berechtigungen
- Einholung und Nachverfolgung von Nutzereinwilligungen (Terms of Use)
- Technische Überprüfung bestimmter Nutzereigenschaften (z.B. Validierung von E-Mail-Adressen)
- Nachnutzung bestehender Nutzerkonten der Heimateinrichtung (DFN-AAI)

Benutzer- und Rechteverwaltung

Roles

Show 10 entries

Search:

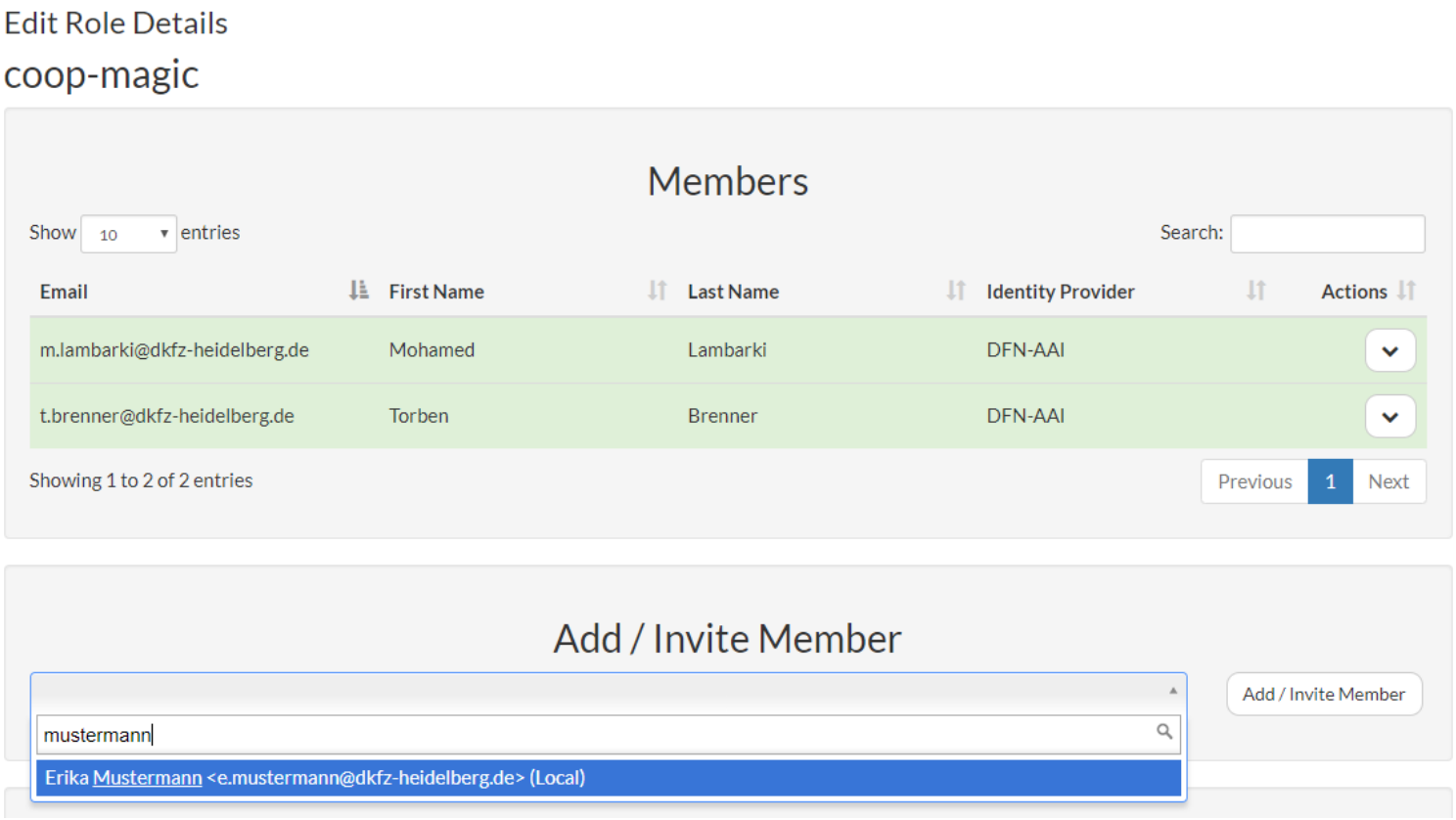
Name	Description	Identifier	Actions
AuthDocs	Dokumentation Samply.Auth	AUTH_DOCS	
Confluence Admin	Admin Gruppe für Confluence	confluence-administrators	
Confluence User	Benutzer Gruppe für Confluence	confluence-users	
coop-magic	Projektpartner MAGIC	coop-magic	
MAGIC	Demo Anwendungen für Projekt MAGIC	MAGIC	

Showing 1 to 5 of 5 entries

Previous 1 Next

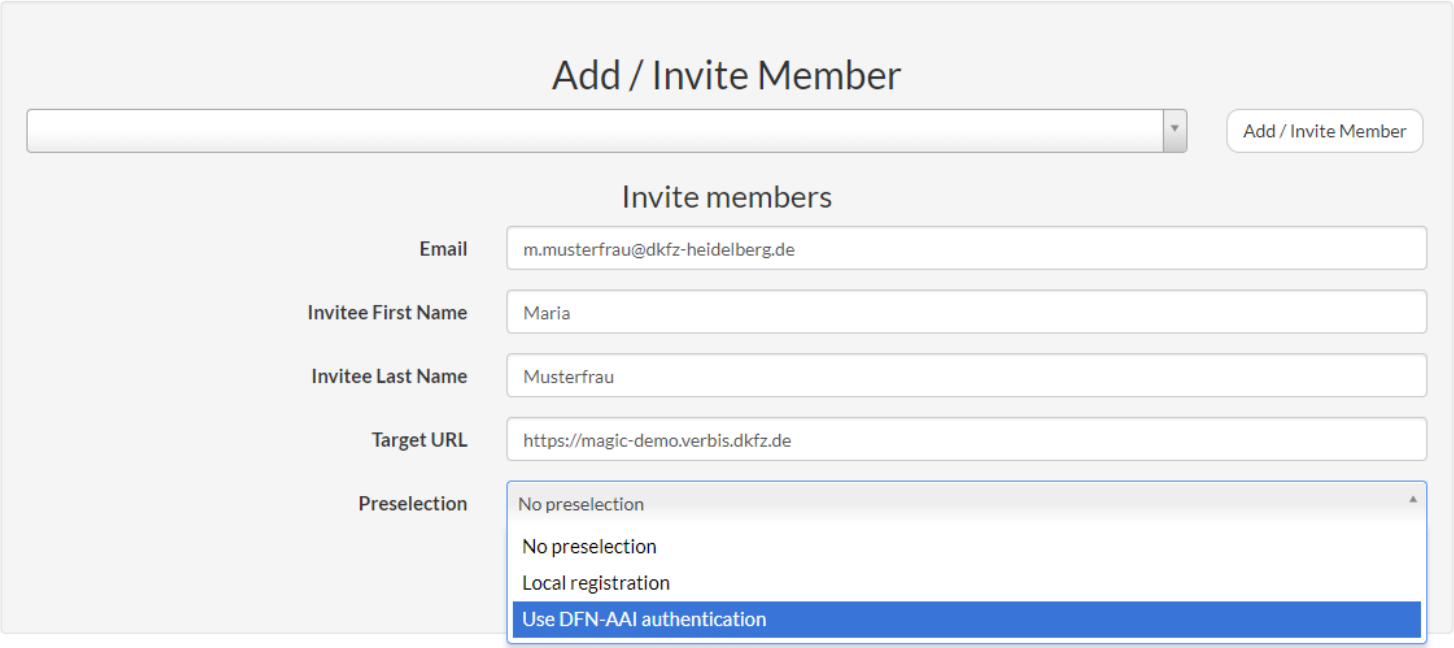
Benutzer- und Rechteverwaltung

- Um einem Benutzer Berechtigungen zu geben, muss er zu einer dafür definierten Rolle hinzugefügt werden



Benutzer- und Rechteverwaltung

- Falls dieser Benutzer noch keinen Account bei Auth Dienst hat, muss man ihn zu Rolle einladen



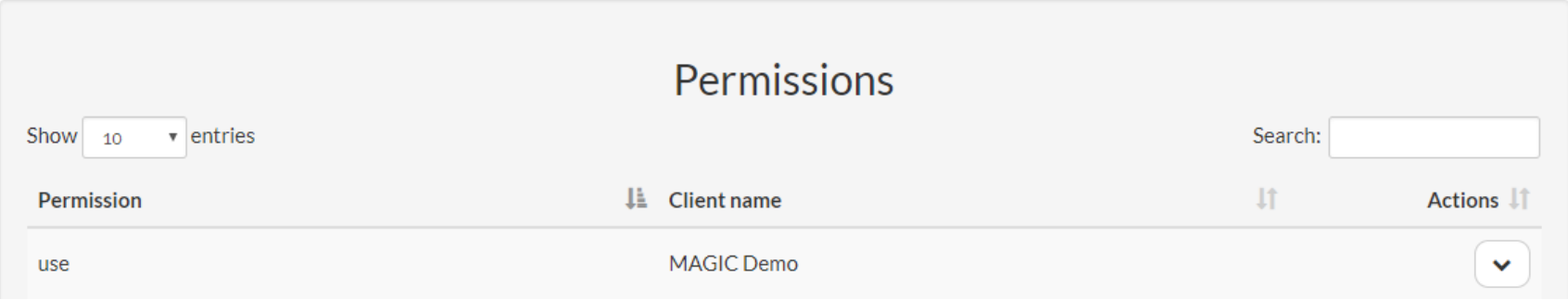
- Auth Dienst versendet an Benutzer eine Email mit Invite Link

Authentifizierungsdienst

- Verwaltung von Benutzern und Berechtigungen
- Zentralisierte Verwaltung der Nutzerberechtigungen von Webanwendungen
- Einholung und Nachverfolgung von Nutzereinwilligungen (Terms of Use)
- Technische Überprüfung bestimmter Nutzereigenschaften (z.B. Validierung von E-Mail-Adressen)
- Nachnutzung bestehender Nutzerkonten der Heimateinrichtung (DFN-AAI)

Nutzerberechtigungen von Webanwendungen

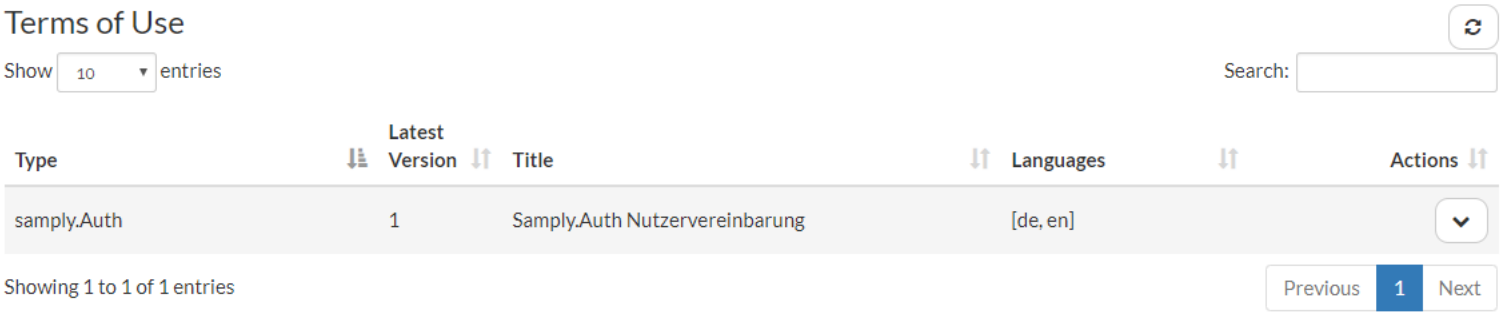
- Zentralisierte Verwaltung der Nutzerberechtigungen von Webanwendungen

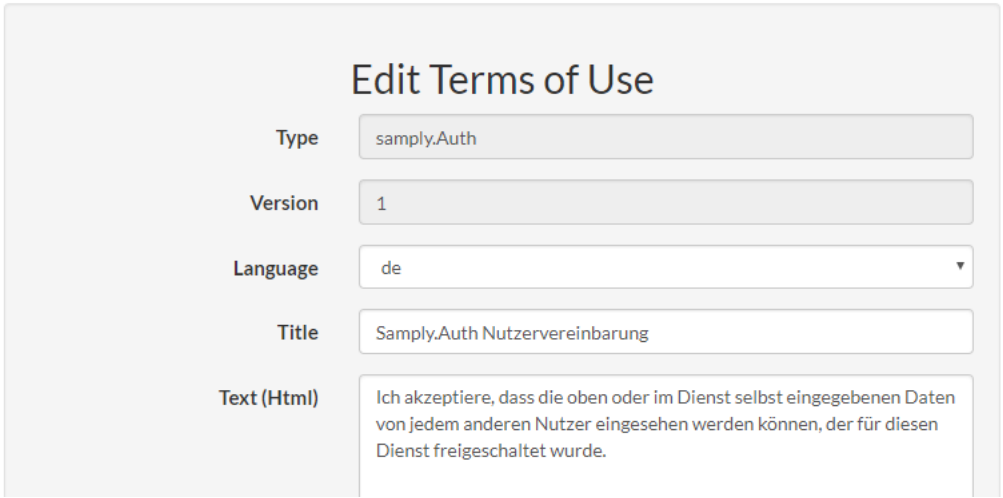


Authentifizierungsdienst

- Verwaltung von Benutzern und Berechtigungen
- Zentralisierte Verwaltung der Nutzerberechtigungen von Webanwendungen
- Einholung und Nachverfolgung von Nutzereinwilligungen (Terms of Use)
- Technische Überprüfung bestimmter Nutzereigenschaften (z.B. Validierung von E-Mail-Adressen)
- Nachnutzung bestehender Nutzerkonten der Heimateinrichtung (DFN-AAI)

Terms of Use

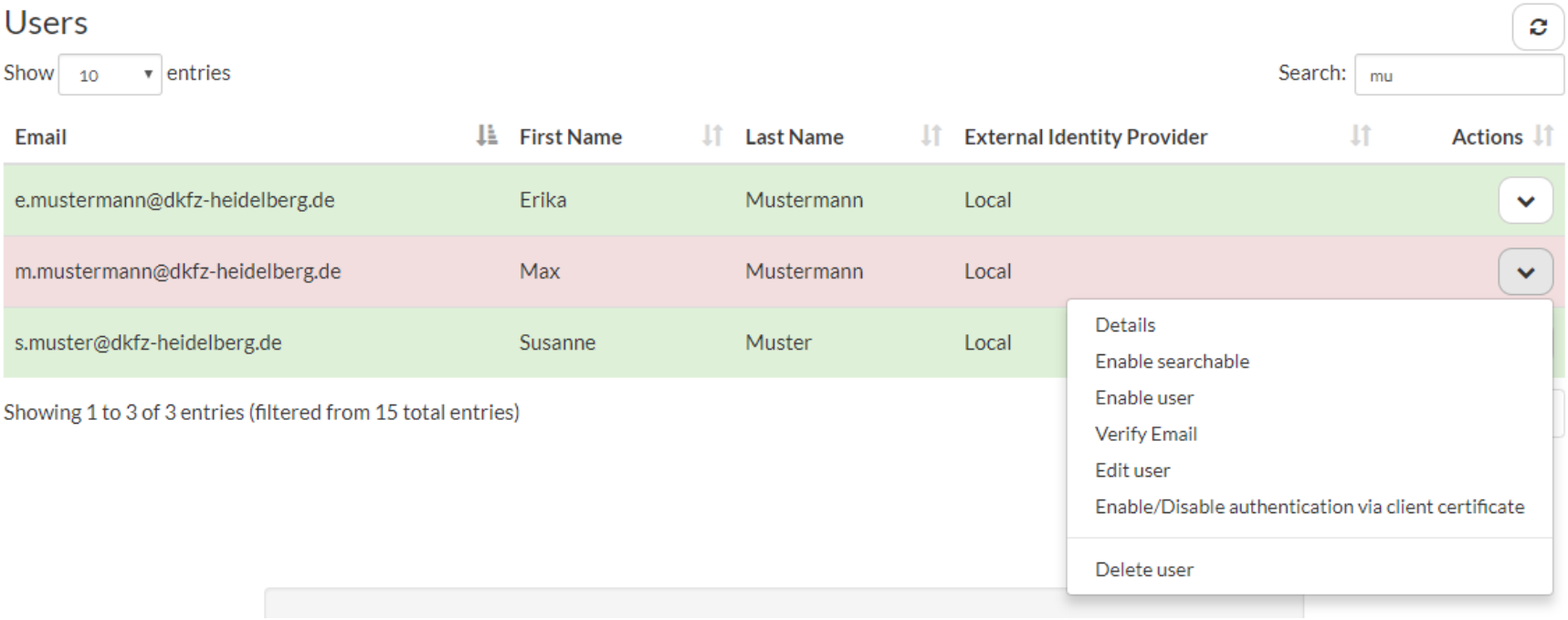

Terms of Use
Show 10 entries
Search:
Type
Latest Version
Title
Languages
Actions
samply.Auth
1
Samply.Auth Nutzervereinbarung
[de, en]
Showing 1 to 1 of 1 entries
Previous
1
Next


Edit Terms of Use
Type
samply.Auth
Version
1
Language
de
Title
Samply.Auth Nutzervereinbarung
Text (Html)
Ich akzeptiere, dass die oben oder im Dienst selbst eingegebenen Daten von jedem anderen Nutzer eingesehen werden können, der für diesen Dienst freigeschaltet wurde.

Authentifizierungsdienst

- Verwaltung von Benutzern und Berechtigungen
- Zentralisierte Verwaltung der Nutzerberechtigungen von Webanwendungen
- Einholung und Nachverfolgung von Nutzereinwilligungen (Terms of Use)
- Technische Überprüfung bestimmter Nutzereigenschaften (z.B. Validierung von E-Mail-Adressen)
- Nachnutzung bestehender Nutzerkonten der Heimateinrichtung (DFN-AAI)

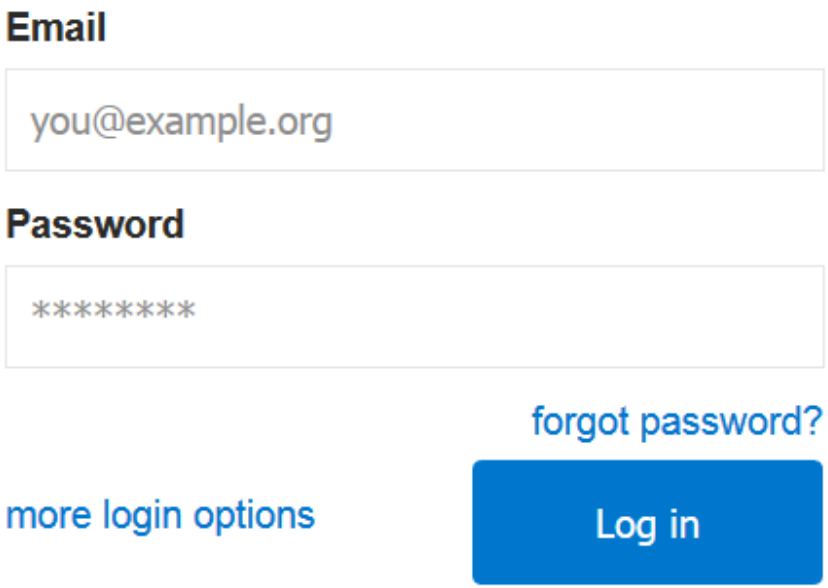
Überprüfung der Nutzereigenschaften



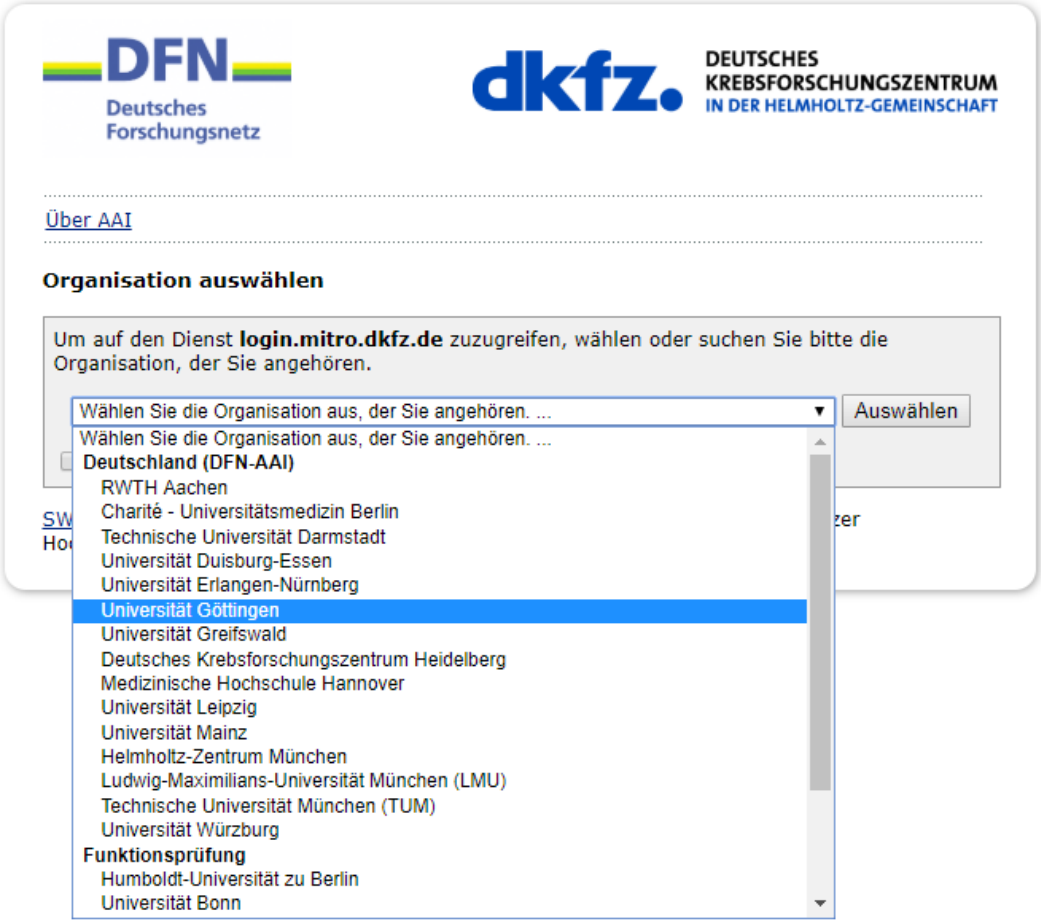
Authentifizierungsdienst

- Verwaltung von Benutzern und Berechtigungen
- Zentralisierte Verwaltung der Nutzerberechtigungen von Webanwendungen
- Einholung und Nachverfolgung von Nutzereinwilligungen (Terms of Use)
- Technische Überprüfung bestimmter Nutzereigenschaften (z.B. Validierung von E-Mail-Adressen)
- Nachnutzung bestehender Nutzerkonten der Heimateinrichtung (DFN-AAI)

Authentifizierung von Nutzern

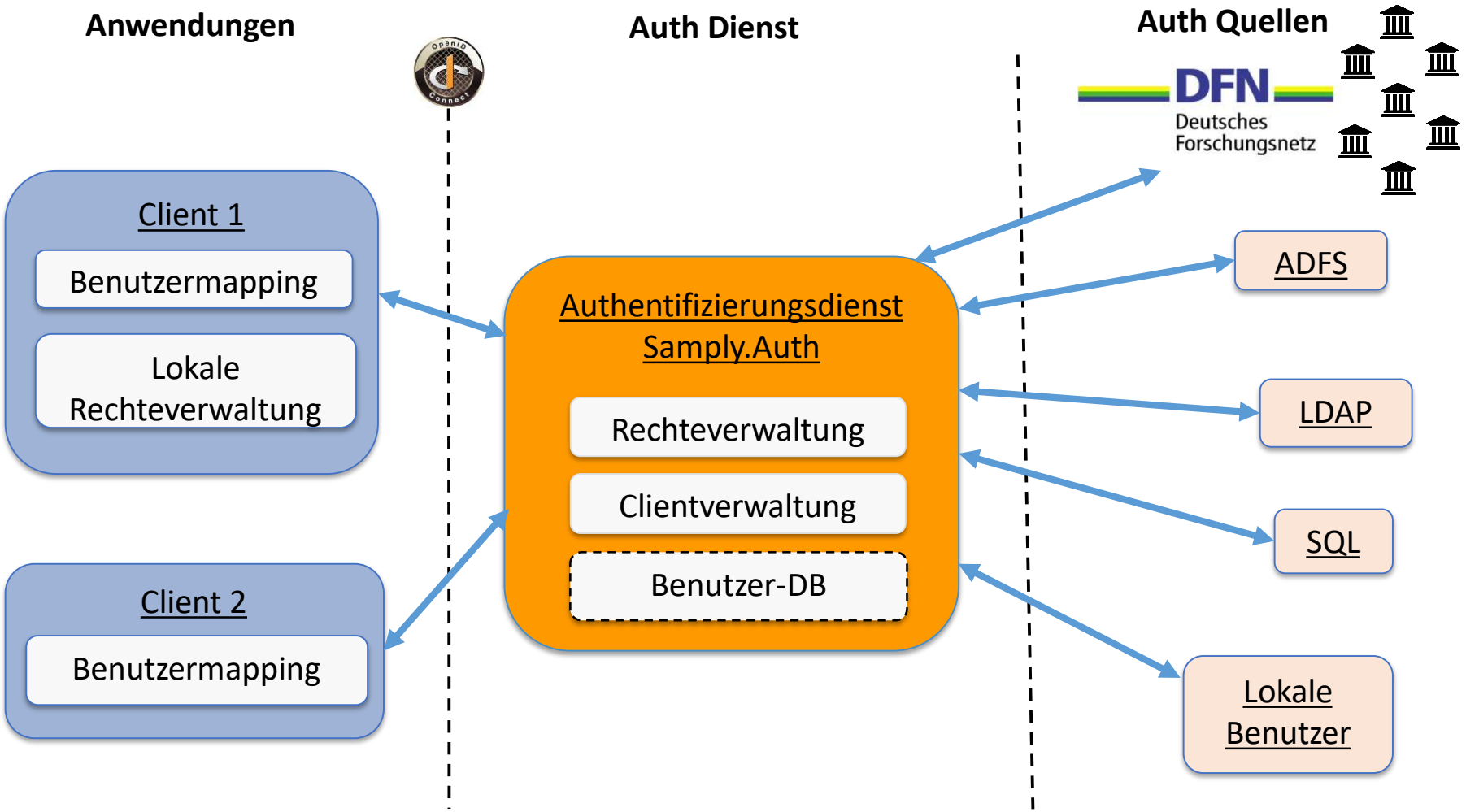


Authentifizierung von Nutzern (DFN-AAI)



Authentifizierung von Nutzern (DFN-AAI)

Authentifizierung von Nutzern: Implementierung



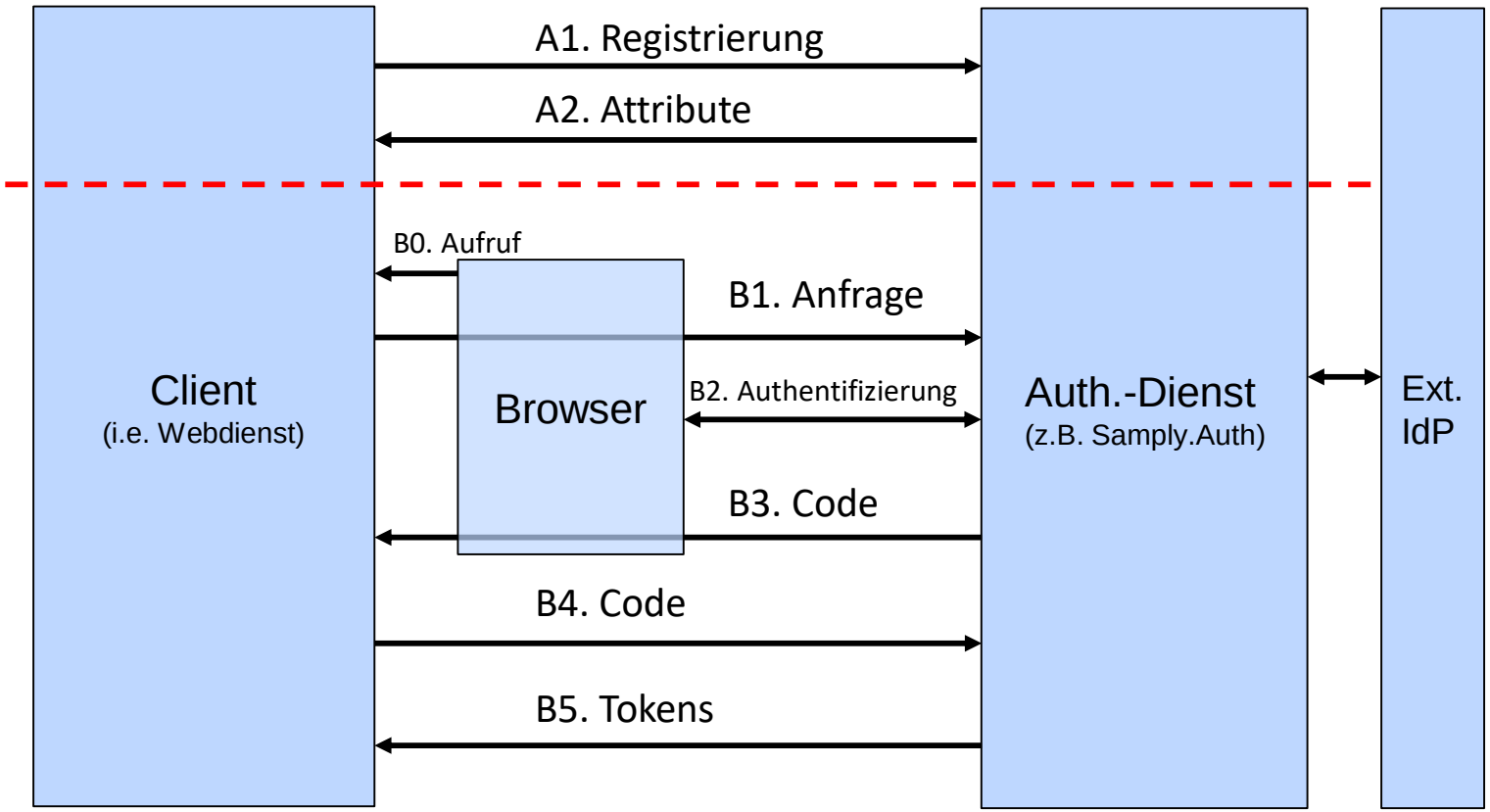
Externe Identity Provider

- **LDAP** (*Lightweight Directory Access Protocol*) - Ein Verzeichnisdienst stellt bestimmte Daten (Benutzeridentitäten) zur Verfügung, die hierarchisch aufgebaut sind und sich verteilt in einem Netzwerk befinden können.
- **ADFS** (*Active Directory Federation Services*) - Software von Microsoft für die organisationsübergreifende Anmeldung, welche nutzt die Benutzerverwaltung des Active Directories (AD)
- **DFN-AAI** (Shibboleth Identity Provider) - Authentifizierungs- und Autorisierungs-Infrastruktur für wissenschaftliche Einrichtungen (Universitäten, Institute) und Anbieter (kommerziell und nicht kommerziell)
- **SQL** - Verwendung von Benutzerkonten aus bestehenden SQL Datenbanken

Samply.Auth: Installation und Konfiguration

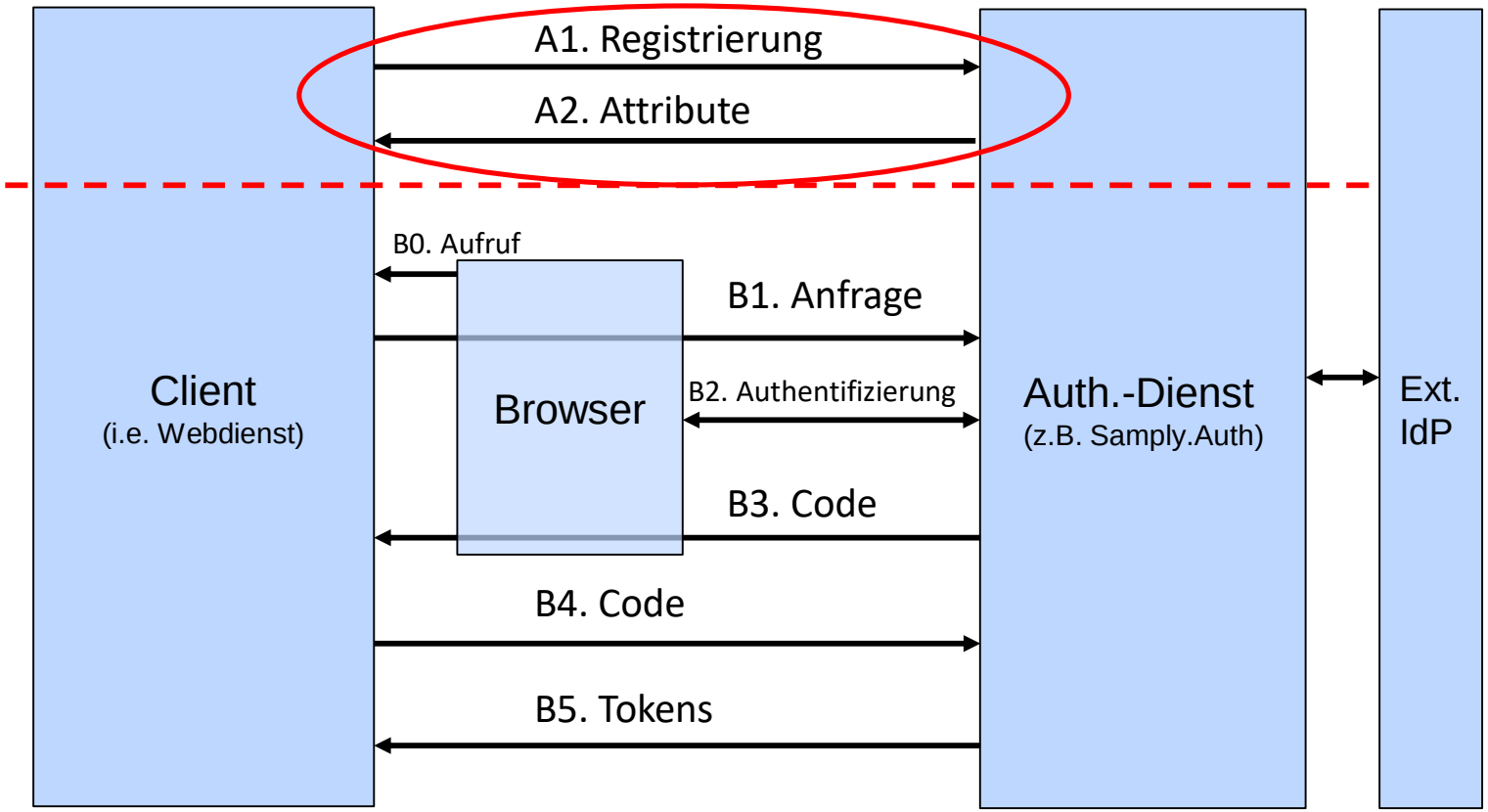
- Docker Container für Samply.Auth (bald verfügbar):
  https://bitbucket.org/medicalinformatics/samply.auth.webapp.docker/
- Docker Konfigurationsdatei (samply.auth.config):
  - Konfigurationen für Datenbank, Netzwerk, Zugriff zur Admin-Oberfläche und Anbindung an DFN-AAI
- Kann sowohl für Samply.Auth als auch für Samply.Auth mit einem Shibboleth Identity Provider und WAYF Dienst verwendet werden

Anbindung eines Webdienstes an Auth Dienst



Zu implementieren durch Webdienst

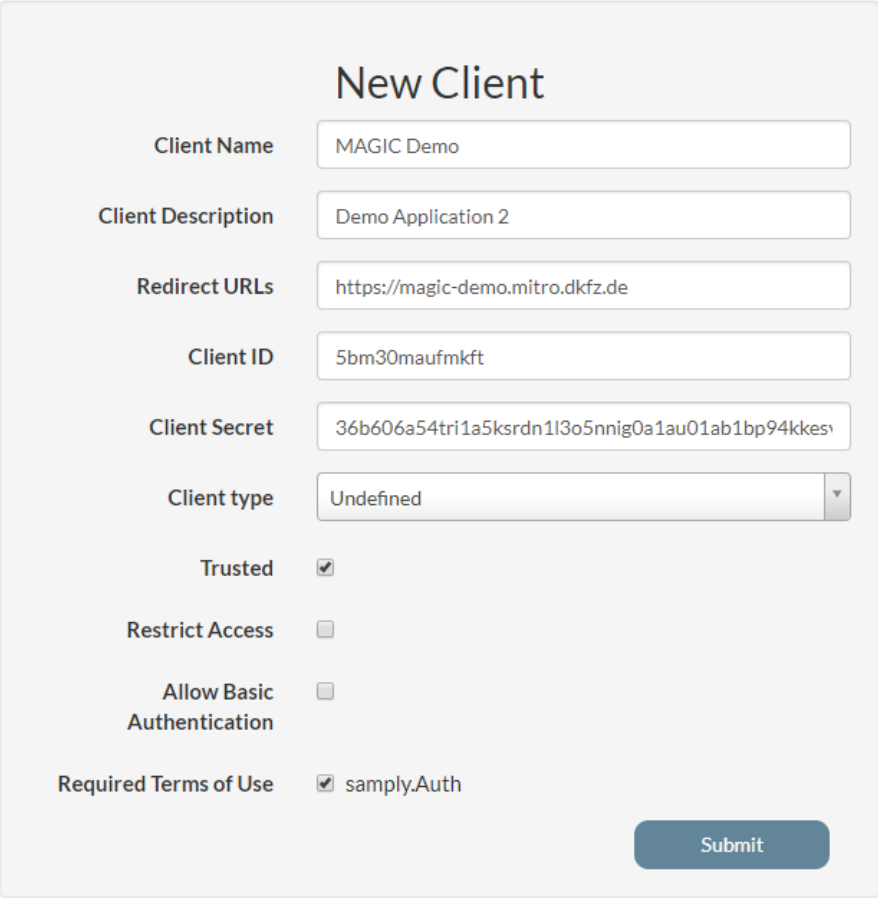
Anbindung eines Webdienstes an Auth Dienst



B6. Validierung Tokens

Beispiel-Ablauf anhand Samply.Auth

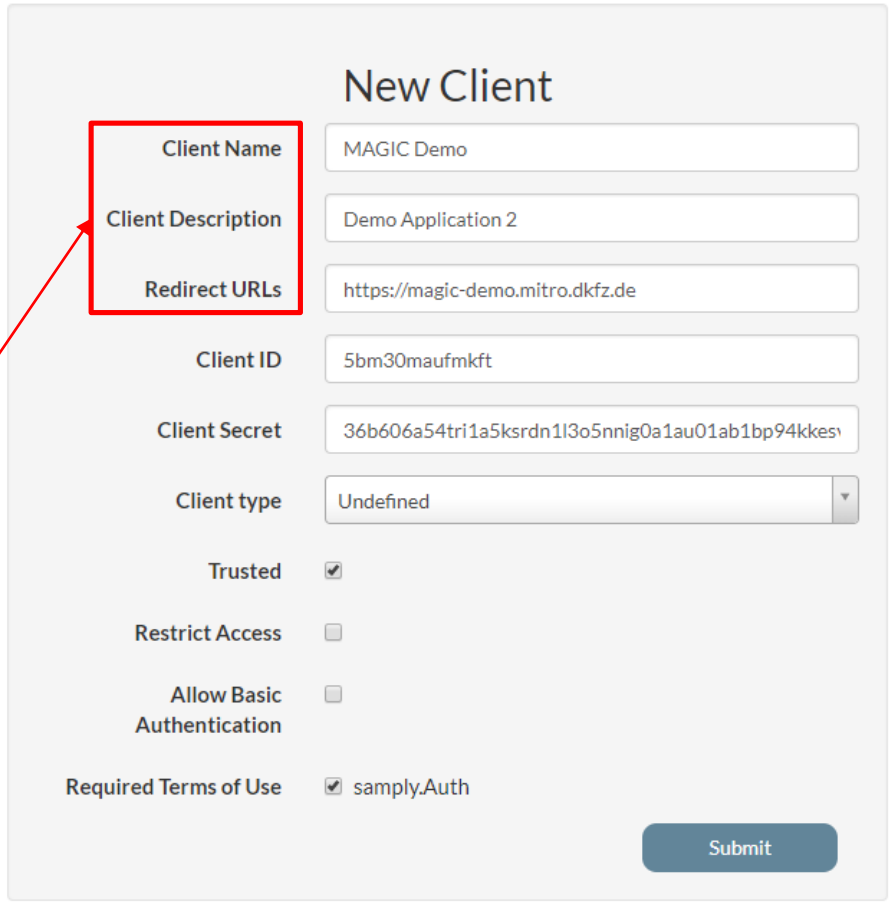
A1. Auth-Admin bittet um Eintragung des Clients (via Web-GUI, s.u.)



Beispiel-Ablauf anhand Samply.Auth

A1. Auth-Admin bittet um Eintragung des Clients (via Web-GUI, s.u.)

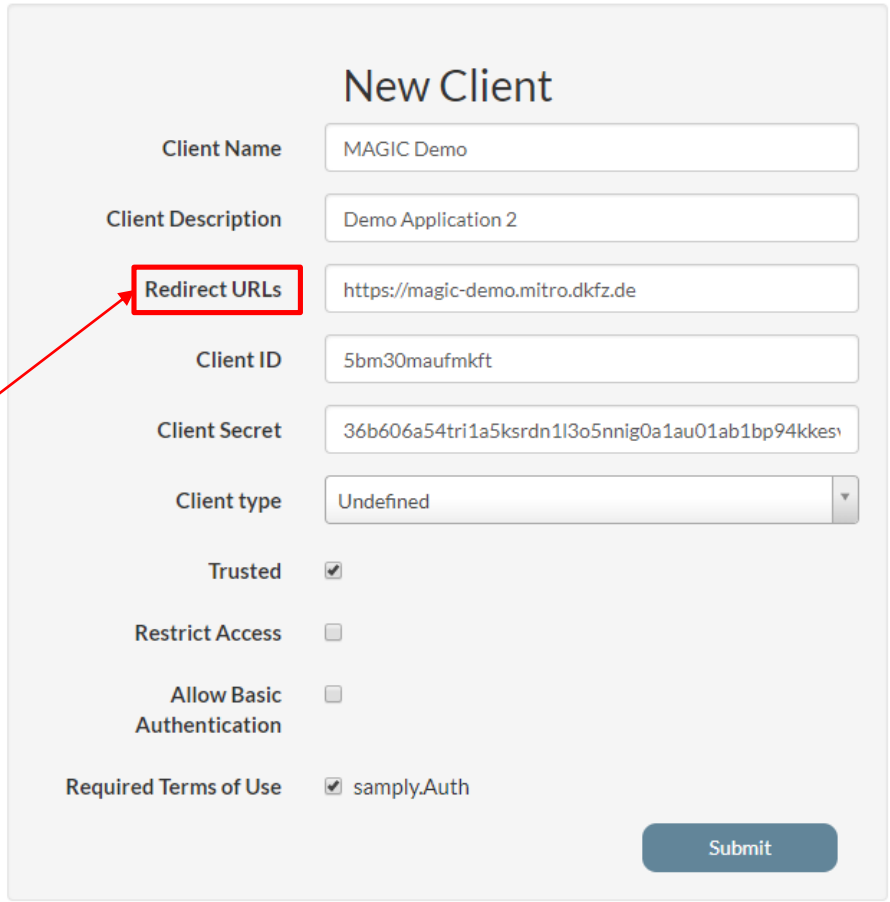
Notwendige Eingaben für Registrierung eines Clients



Beispiel-Ablauf anhand Samply.Auth

A1. Auth-Admin bittet um Eintragung des Clients (via Web-GUI, s.u.)

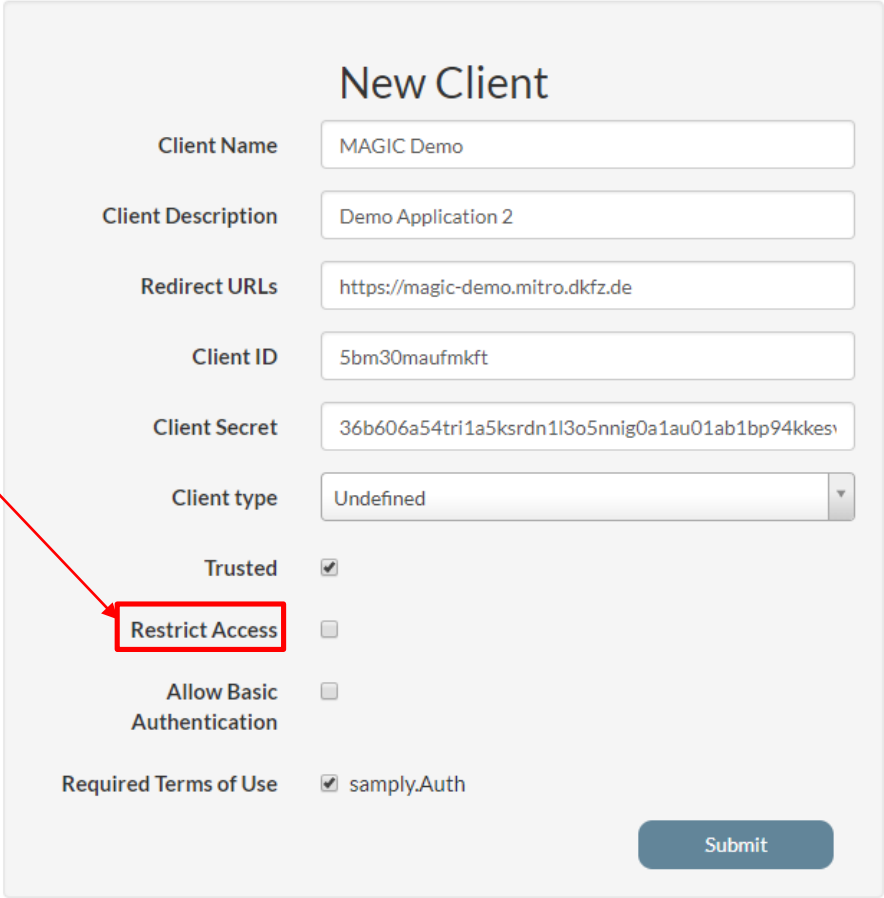
URLs für die Validierung der redirect URLs



Beispiel-Ablauf anhand Samply.Auth

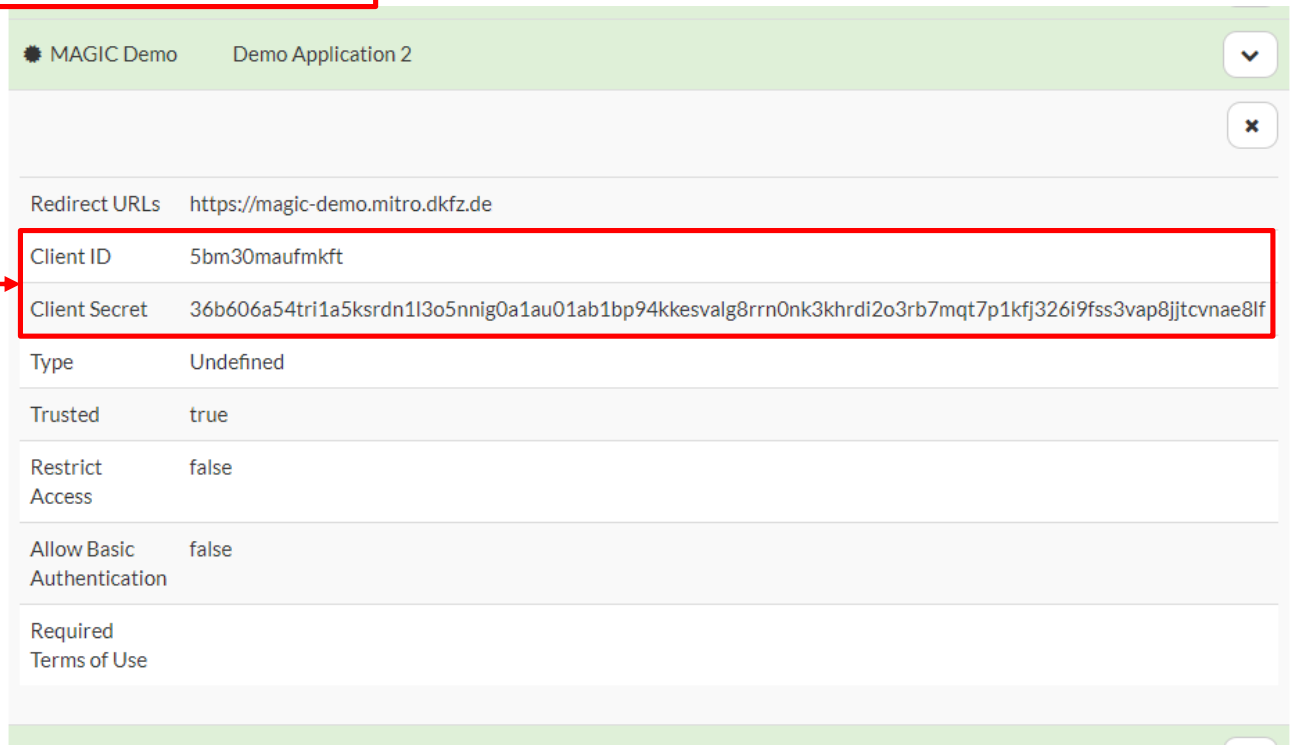
A1. Auth-Admin bittet um Eintragung des Clients (via Web-GUI, s.u.)

True:
Zugriff nur für berechtigte Benutzer
False:
Zugriff für alle



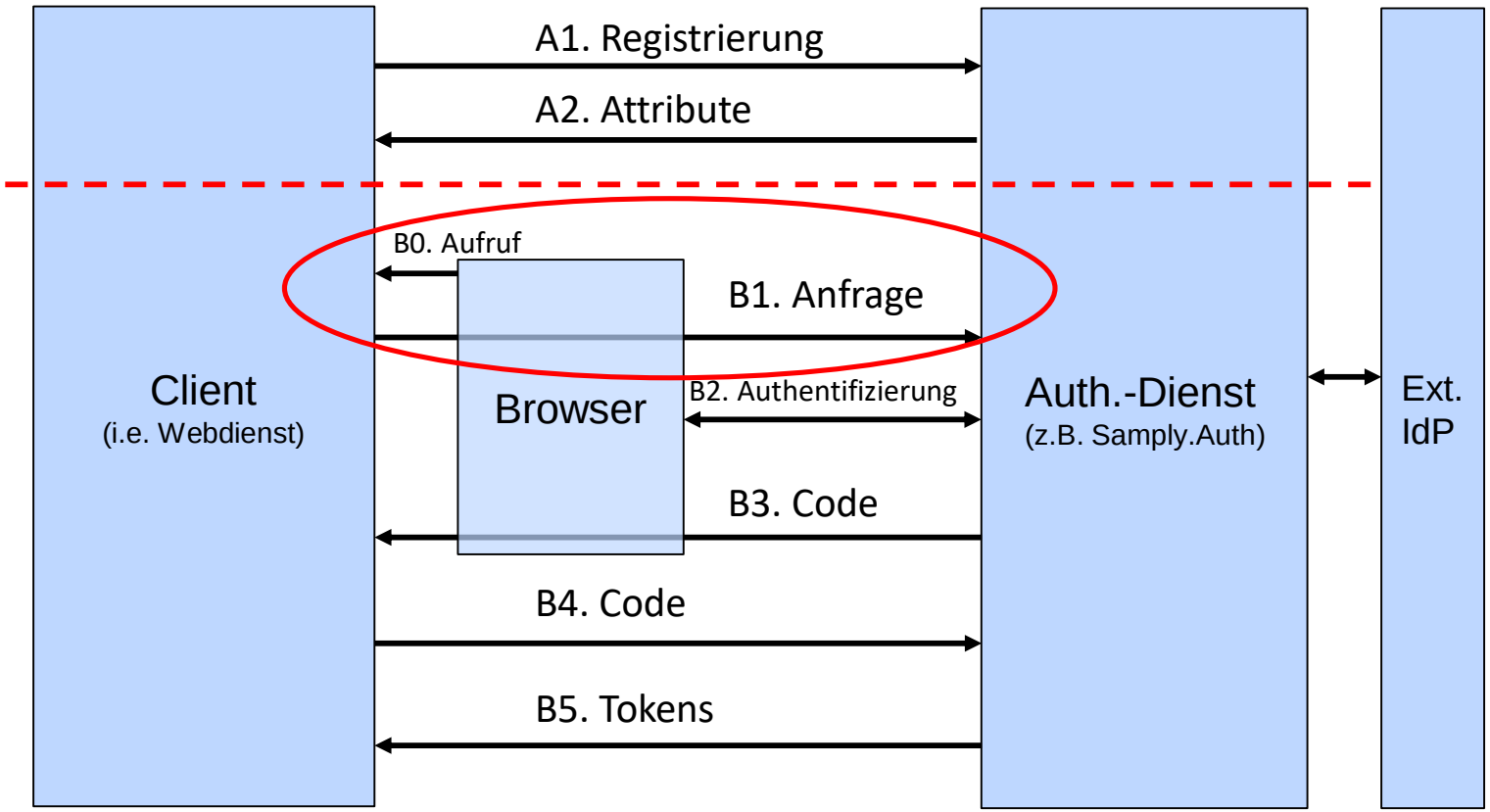
Beispiel-Ablauf anhand Samply.Auth

A2. Antwort von Auth-Admin:
Client ID, Client Secret, Auth Base URL



Public Key: https://login.verbis.dkfz.de/oauth2/certs

Anbindung eines Webdienstes an Auth Dienst



B6. Validierung Tokens

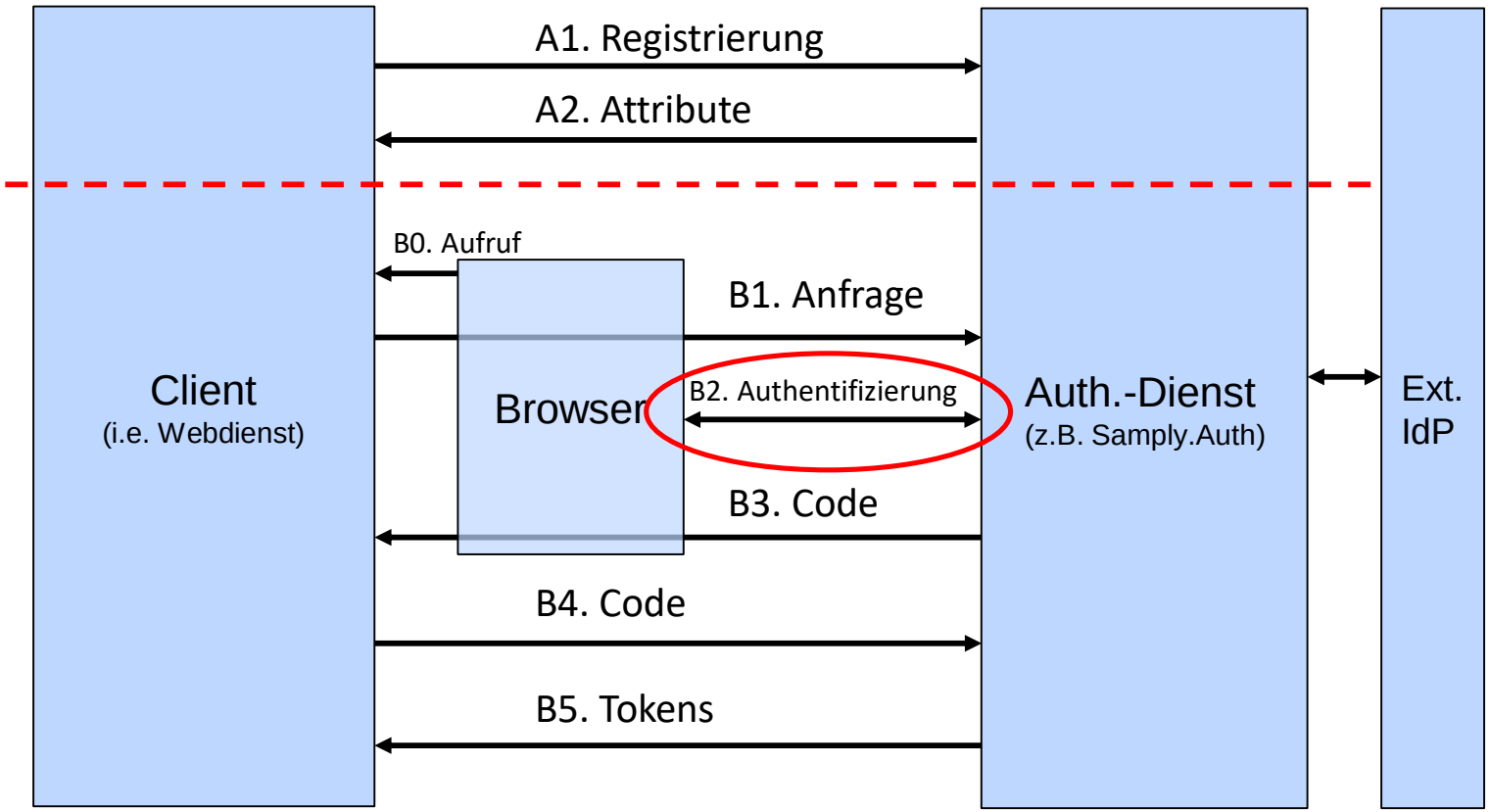
Beispiel-Ablauf anhand Samply.Auth

B0. Nutzer besucht den Client mit seinem Browser. Client stellt fest, dass Nutzer authentifiziert werden muss.

B1. Client redirected Browser an Samply.Auth

https://login.verbis.dkfz.de/auth/grant.xhtml
?client_id=5bm30maufmkft
&redirect_uri=https%3A%2F%2Fmagic-demo.mitro.dkfz.de
&scope=openid
&state=af0ifjsldkj

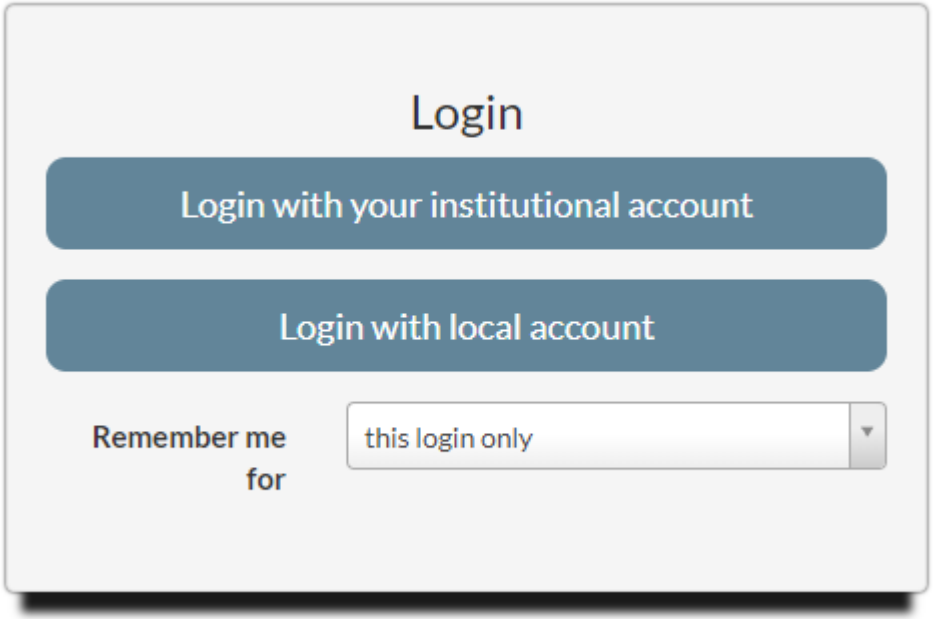
Anbindung eines Webdienstes an Auth Dienst



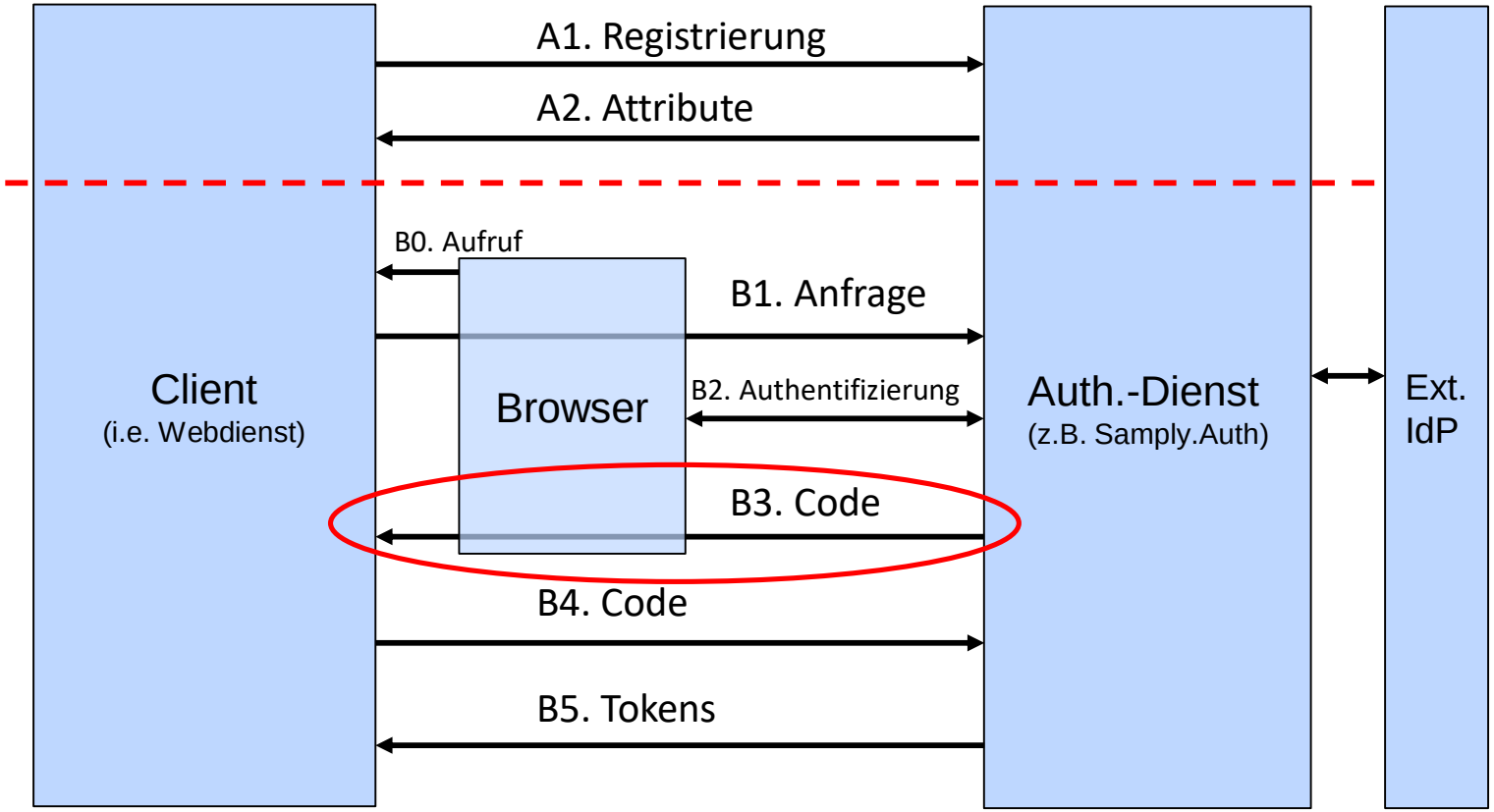
B6. Validierung Tokens

Beispiel-Ablauf anhand Samply.Auth

B2. (Samply.Auth authentifiziert Nutzer gegen einen IdP)



Anbindung eines Webdienstes an Auth Dienst



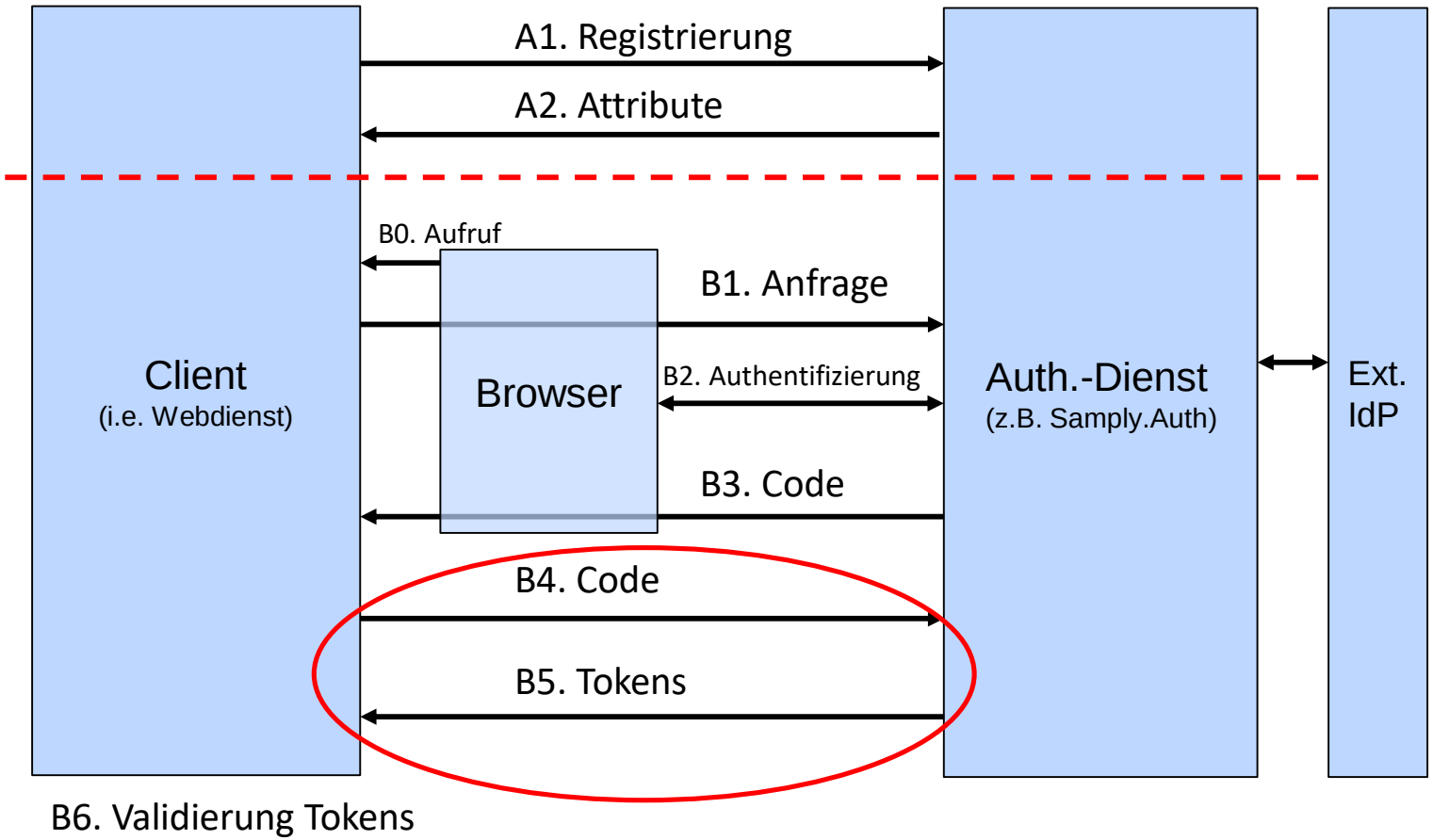
B6. Validierung Tokens

Beispiel-Ablauf anhand Samply.Auth

B3. Samply.Auth redirected Browser zurück zu Client:

https://magic-demo.mitro.dkfz.de/
?code=3i4oshd8249a[…]ft08fogitfs5n2
&state=af0ifjsldkj

Anbindung eines Webdienstes an Auth Dienst



Beispiel-Ablauf anhand Samply.Auth

B4. Client löst den Code bei Samply.Auth ein…

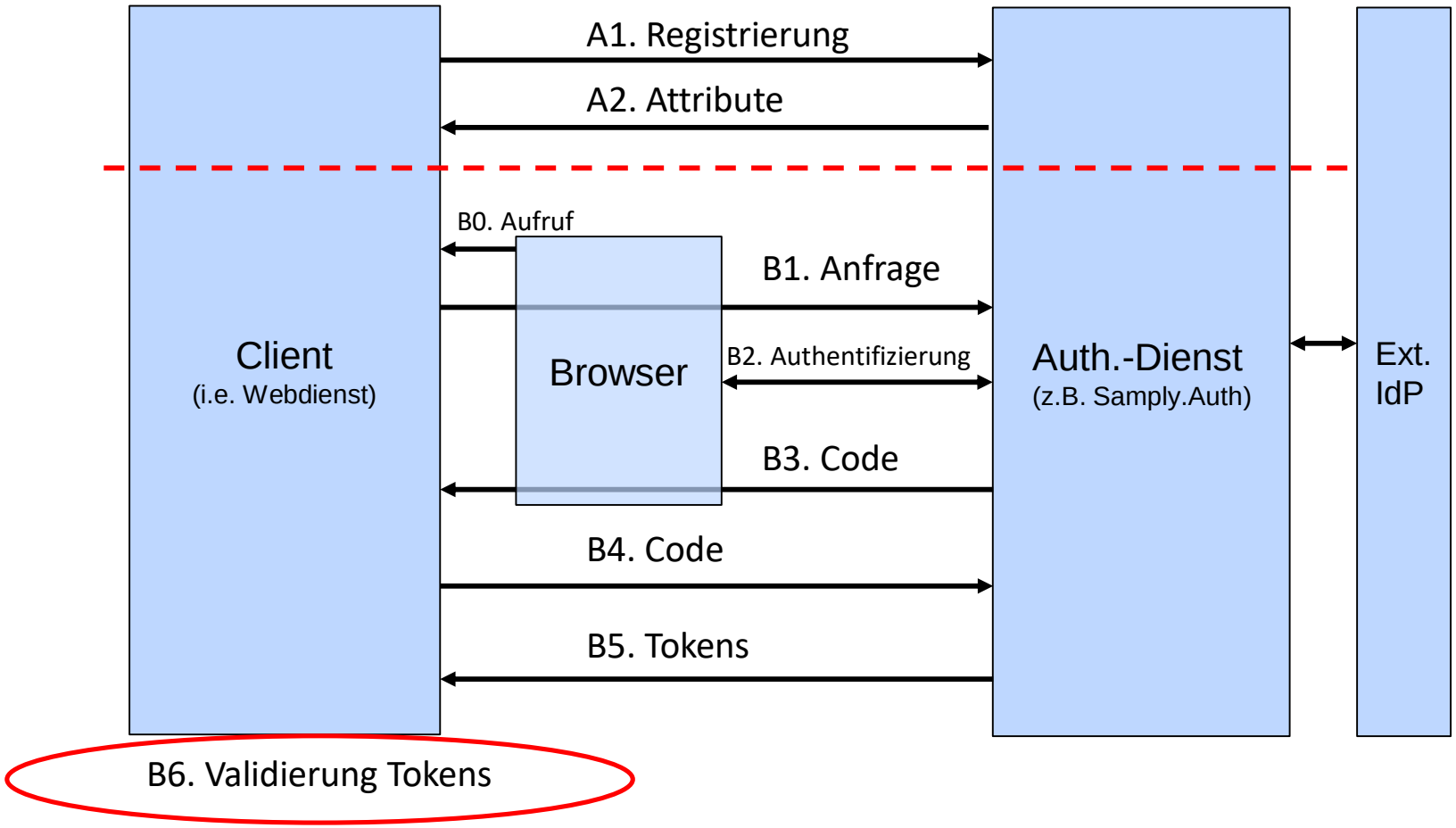
POST https://login.verbis.dkfz.de/auth/oauth2/token

```
{
  "code" : "3i4oshd8249a[…]ft08fogitfs5n2 ",
  "client_id" : "5bm30maufmkft",
  "client_secret" : "36b606a[…]3vap8jjtcvnae8lf"
}
```

B5. …und erhält zurück: {ID,Access,Refresh} Token.

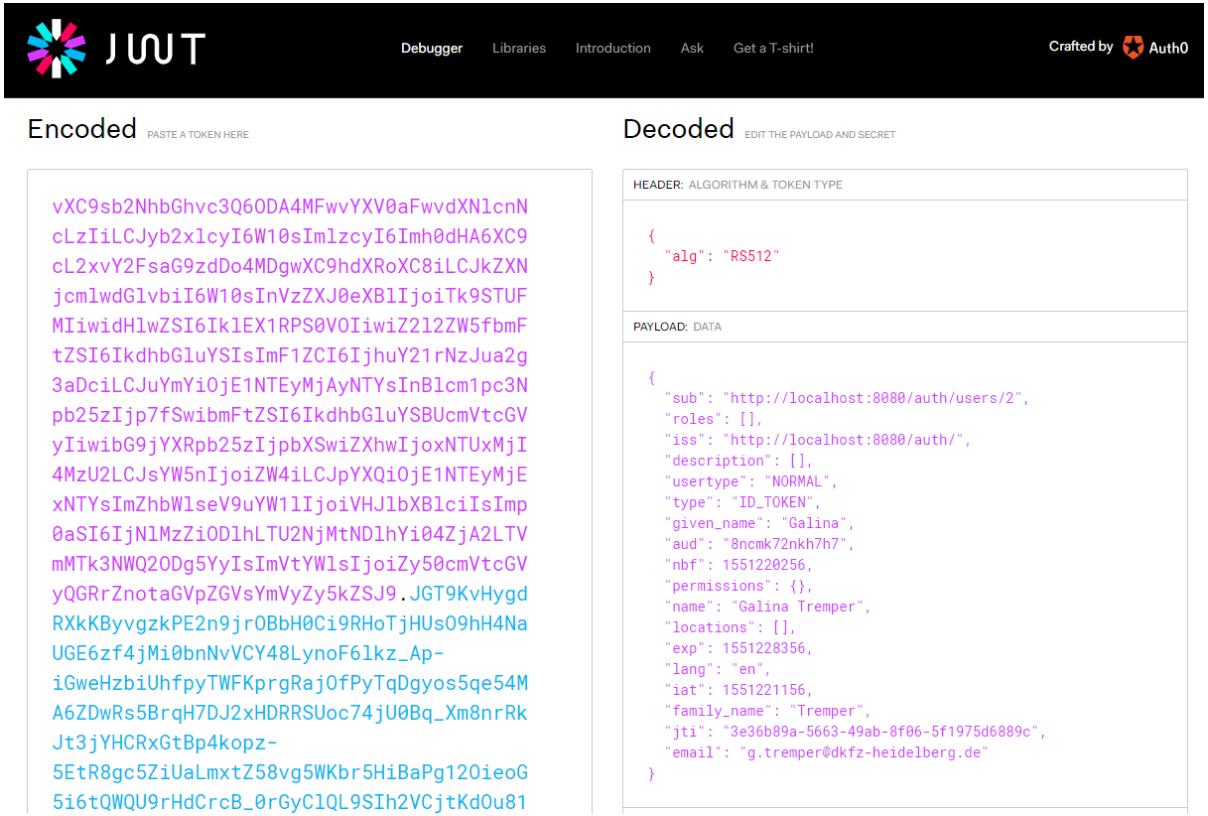
```
{
 "access_token" : "eyJhbG[…]miKeNDI",
 "id_token" : "eyJhbG[…]iG6C2I",
 "refresh_token" : "36b606a[…]dxXOULg ",
 "token_type" : "Bearer",
 "expires_in" : 7200
}
```

Anbindung eines Webdienstes an Auth Dienst



Beispiel-Ablauf anhand Samply.Auth

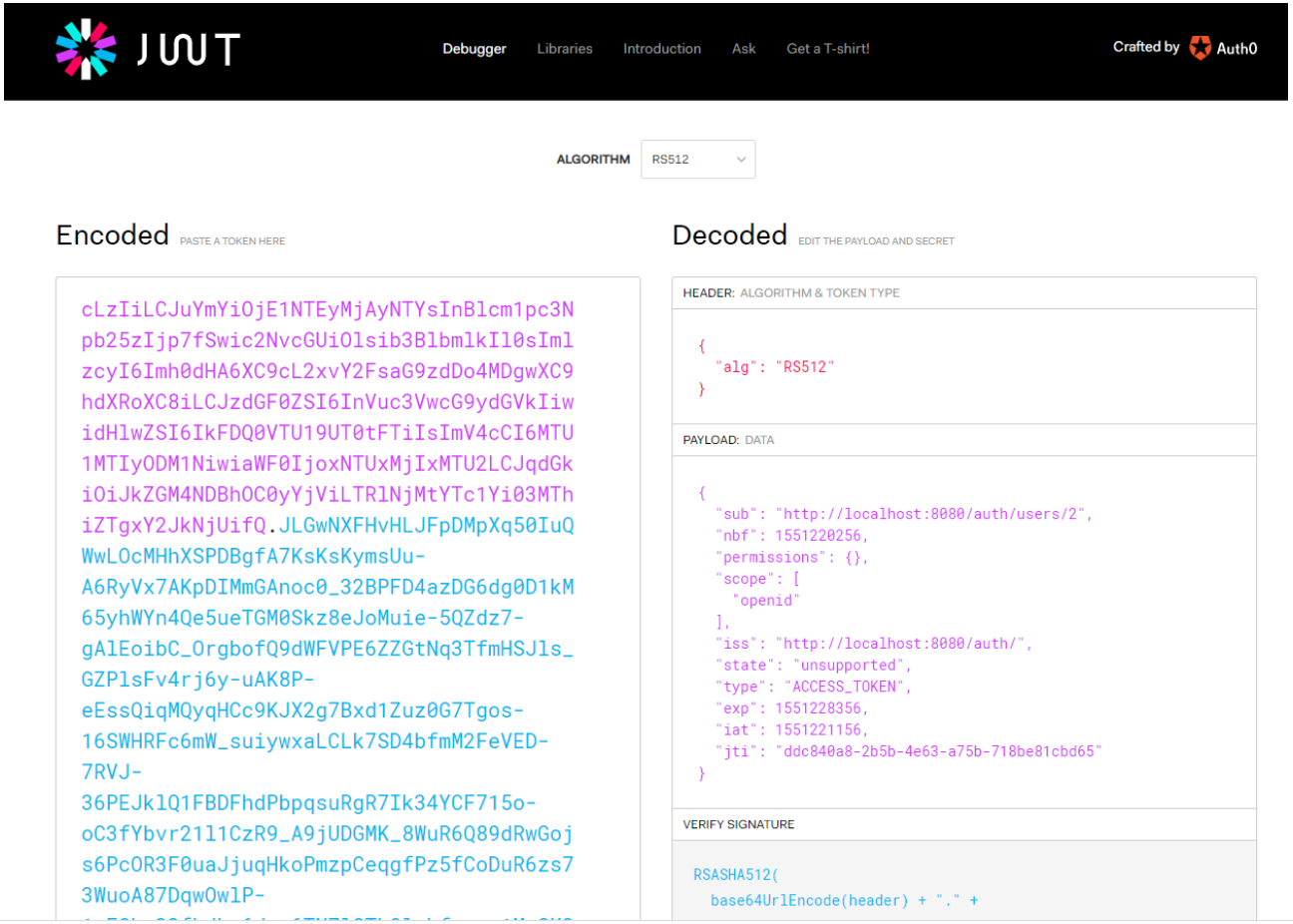
B6. Client entschlüsselt ID-Token (via JWT-Library) und bekommt Benutzer UID, Rollen, …



jwt.io

Beispiel-Ablauf anhand Samply.Auth

Access Token



jwt.io

Föderierte Authentifizierung

- Ca. 270 Identity Provider und ca. 250 Service Provider
- Service-Provider in der DFN-AAI-Basic-Föderation:

https://www.aai.dfn.de/verzeichnis/sp-dfn-aai-basic/

  - Notwendige und optionale Attribute für jeden Service Provider
  - Kontaktpersonen
- Identity-Provider in der DFN-AAI-Basic-Föderation:

https://www.aai.dfn.de/verzeichnis/idp-dfn-aai/

Föderierte Authentifizierung

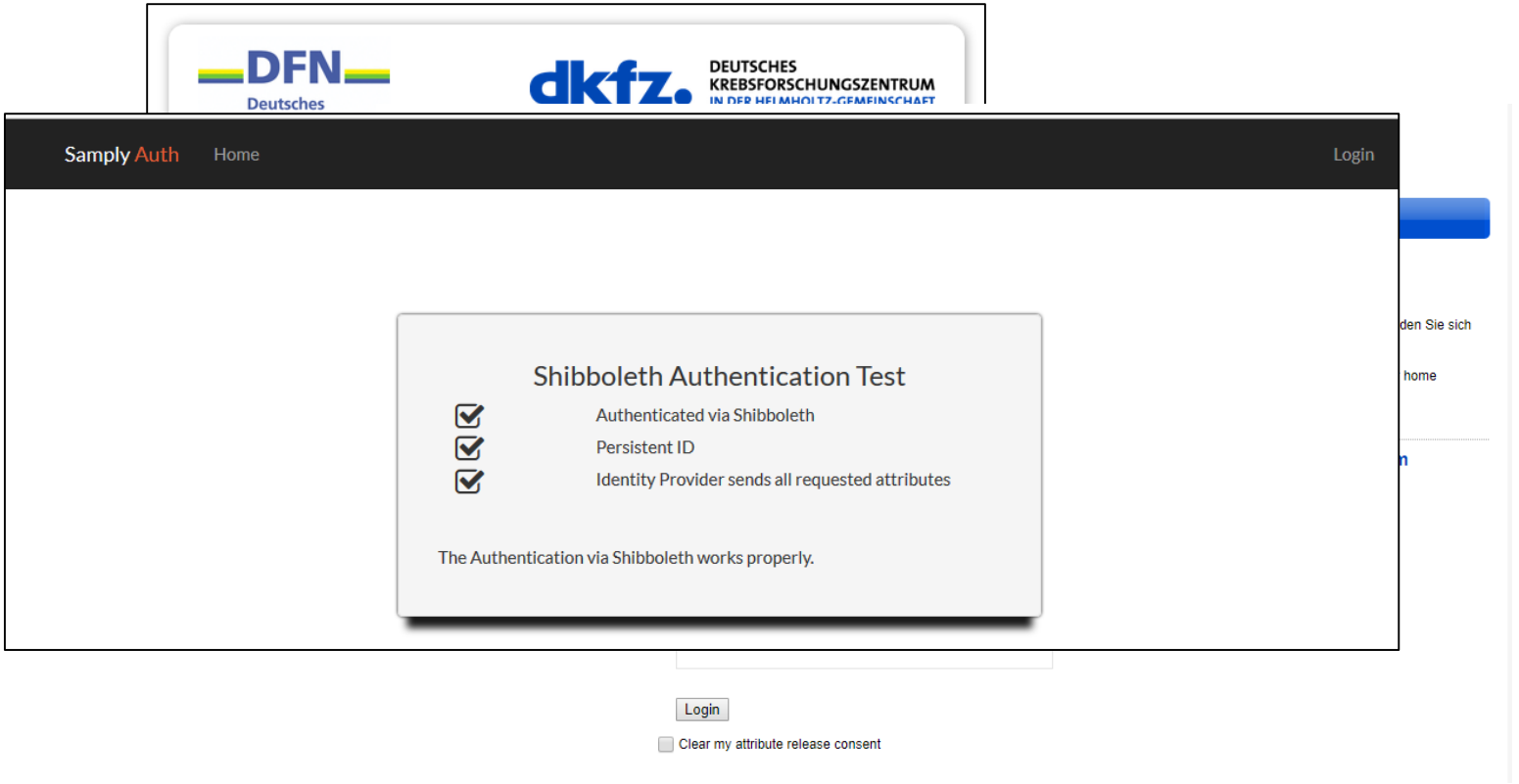
- Attribute für die erfolgreiche Anmeldung in Samply.Auth:
  - SAML persistent identifier (minimale Voraussetzung)
  - E-Mail
  - Vorname, Nachname
- Freigabe der gewünschten Attribute erfolgt nicht automatisch

Test für erfolgreiche Anbindung:

https://login.verbis.dkfz.de/shibbolethTest.xhtml

Praxisbeispiel föderierte Authentifizierung

- Anmeldung erfolgreich (Freigabe aller gewünschten Attribute oder mindestens Persistent ID))



Praxisbeispiel föderierte Authentifizierung

- Ablehnung (Nur *affiliation* wurde freigegeben: *staff@dkfz-heidelberg.de*)
  - IdP direkt kontaktieren

Mail zur Freigabe zusätzlicher Attribute

Sehr geehrte Damen und Herren,

wir sind Betreiber des Service Providers (SP) unter https://login.mitro.dkfz.de in der DFN-AAI. Wann immer es geht, ermöglichen wir unseren Forschungspartnern den Login mit Ihren Heimatkonten über die DFN-AAI, anstatt in unseren Systemen neue Accounts anzulegen. Leider funktioniert der Login unserer Projektpartner in <Stadtname> nicht, da Ihr Identity Provider (IdP) mit der entityID <hier entityID einsetzen> nicht die benötigten Attribute überträgt. Die von uns angeforderten Attribute sind:

- *Zwingend* benötigen wir eine für uns faktisch anonyme, persistente ID, um einen wiederkehrenden Nutzer wiederzuerkennen:
  - urn:oasis:names:tc:SAML:2.0:nameid-format:persistent,
  - urn:mace:dir:attribute-def:eduPersonTargetedID oder
  - urn:oid:1.3.6.1.4.1.5923.1.1.1.10
- Wir fordern außerdem einige nicht-anonyme Attribute an, die Nutzern zukünftig eine Selbstregistrierung in unseren Diensten erlauben. Dafür haben wir eine GÉANT-konforme Datenschutzerklärung unter https://login.mitro.dkfz.de/static/privacy_policy.html veröffentlicht.

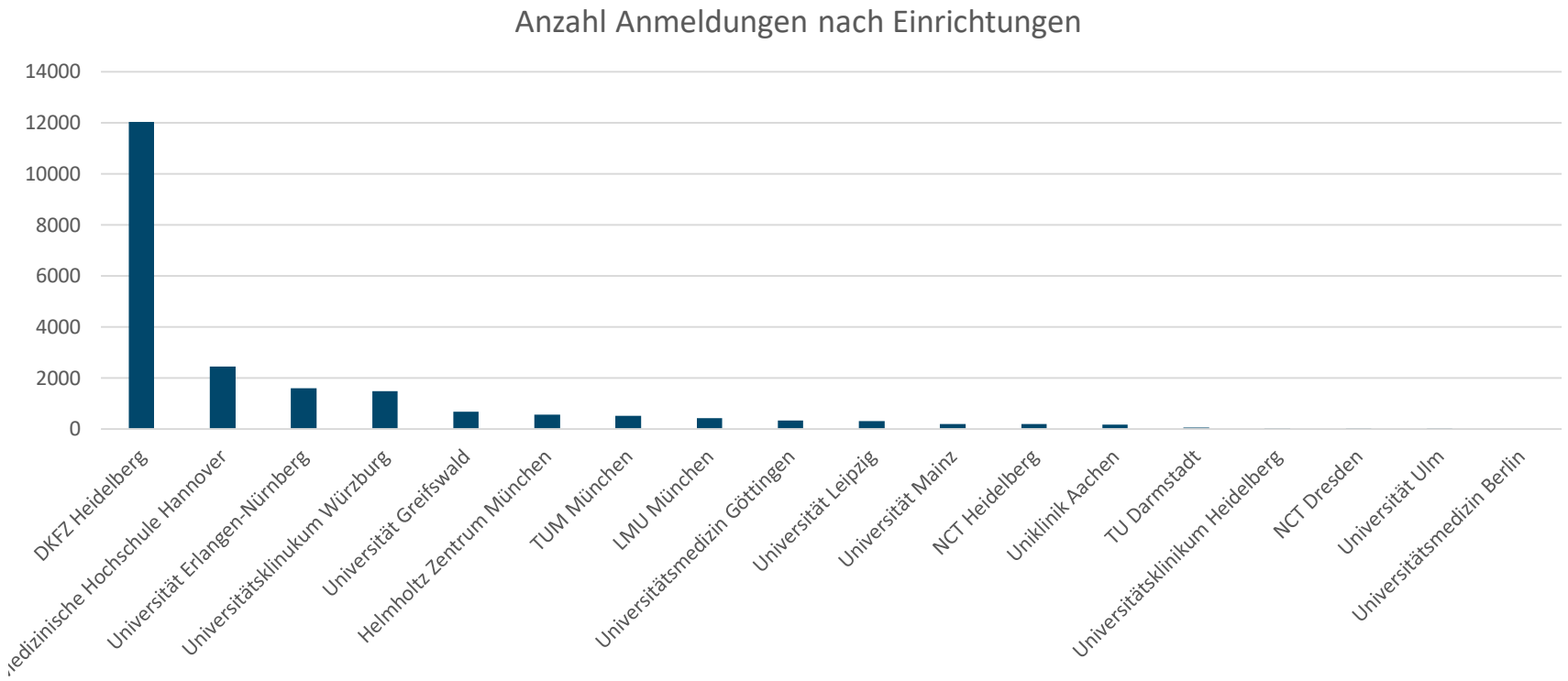
Eine beispielhafte Ergänzung der /etc/shibboleth/attribute-policy.xml Ihres IdP finden Sie im Anhang. Nach Neustart des IdP-Dienstes können Sie unter https://login.mitro.dkfz.de/Shibboleth.sso/Login?target=https%3A%2F%2Flogin.mitro.dkfz.de%2FshibbolethTest.xhtml überprüfen, ob unser SP die nötigen Attribute erhält.

Falls Sie unser Anliegen mit einem Kollegen am Standort besprechen wollen, wenden Sie sich gern an unseren Projektpartner, Herrn Dr. X (mail@domain.de). Für alle anderen Fragen stehen wir natürlich gern zur Verfügung. Vielen Dank für Ihre Unterstützung.

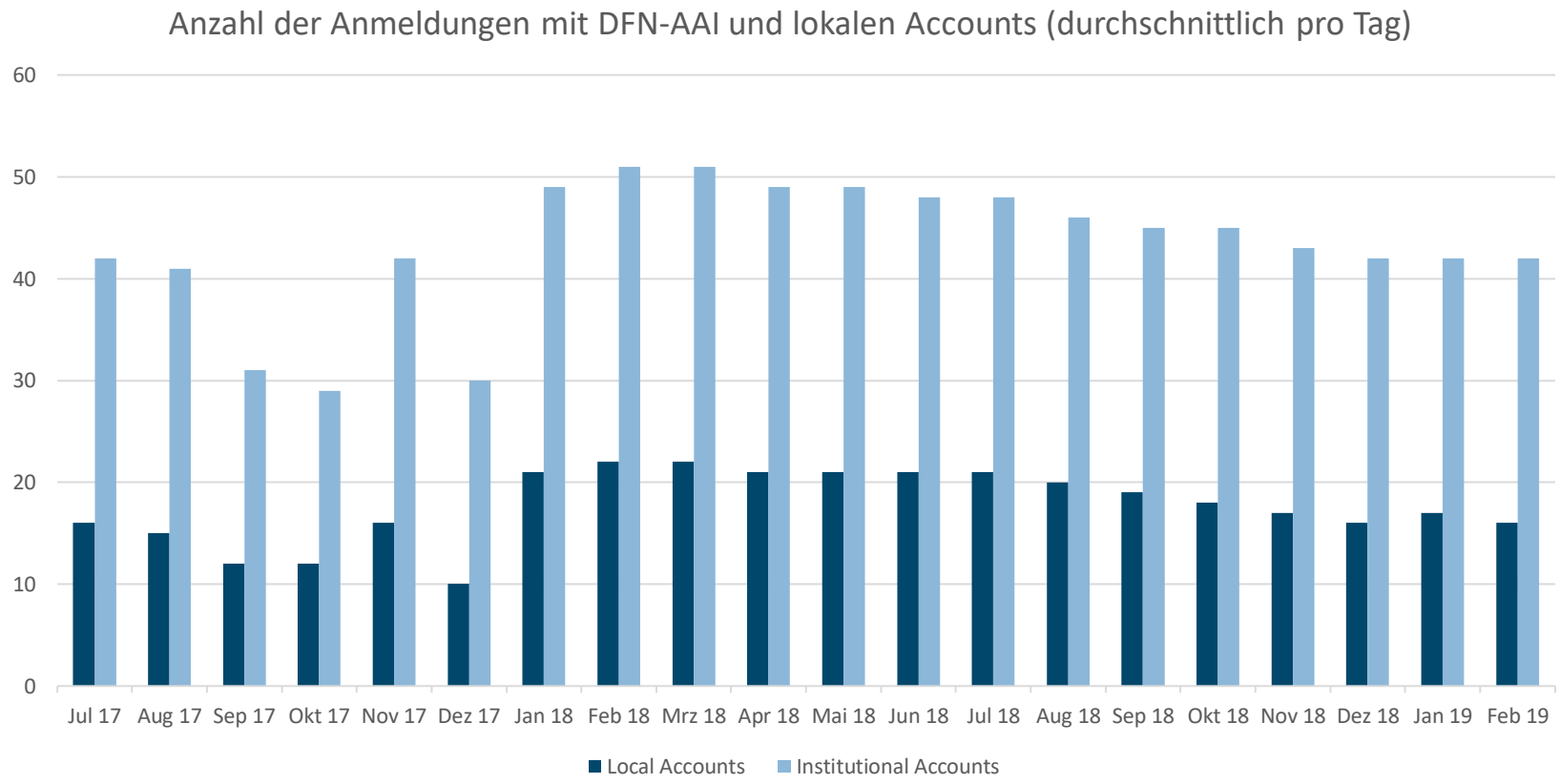
Mit freundlichem Gruß
<Name>

Praxisbeispiel föderierte Authentifizierung

Praxisbeispiel DFN-AAI: Projektalltag am DKFZ
(v.a. DKTK und German Biobank Alliance)



Praxisbeispiel föderierte Authentifizierung



Demo

Veröffentlichung

Danke