

Samply.Auth

MAGIC: IT-Werkzeuge für die medizinische Verbundforschung

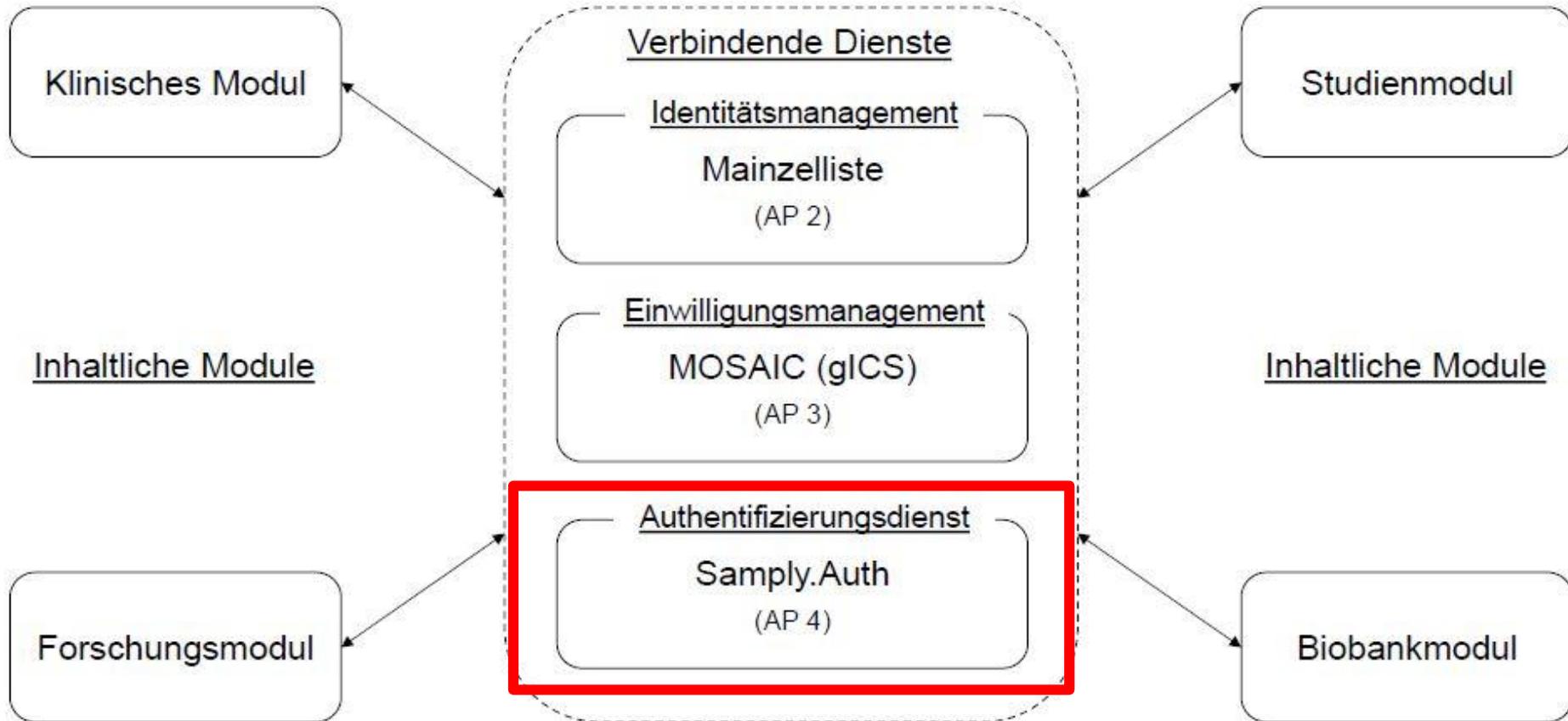
TMF Tutorials | Bonn | 19.03.2019

Galina Tremper

Deutsches Krebsforschungszentrum Heidelberg
Verbundinformationssysteme



Einordnung in den TMF-Leitfaden



- ▶ **Authentifizierung** - 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. Sampil.Auth: Installation und Konfiguration
3. Anbindung an Sampil.Auth - Beispiel-Ablauf
4. Föderierte Authentifizierung
5. Demo

- ▶ 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 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

Edit Role Details
coop-magic

Members

Show entries Search:

Email	First Name	Last Name	Identity Provider	Actions
m.lambarki@dkfz-heidelberg.de	Mohamed	Lambarki	DFN-AAI	▼
t.brenner@dkfz-heidelberg.de	Torben	Brenner	DFN-AAI	▼

Showing 1 to 2 of 2 entries Previous **1** Next

Add / Invite Member

Erika Mustermann <e.mustermann@dkfz-heidelberg.de> (Local)

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

Add / Invite Member

Invite members

Email	<input type="text" value="m.musterfrau@dkfz-heidelberg.de"/>
Invitee First Name	<input type="text" value="Maria"/>
Invitee Last Name	<input type="text" value="Musterfrau"/>
Target URL	<input type="text" value="https://magic-demo.verbis.dkfz.de"/>
Preselection	<div><p>No preselection</p><p>No preselection</p><p>Local registration</p><p>Use DFN-AAI authentication</p></div>

- ▶ Auth Dienst versendet an Benutzer eine Email mit Invite Link

- ▶ 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

Permissions

Show entries Search:

Permission	Client name	Actions
use	MAGIC Demo	<input type="button" value="v"/>

- ▶ 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 entries

Search:



Type	Latest Version	Title	Languages	Actions
sample.Auth	1	Sample.Auth Nutzervereinbarung	[de, en]	<input type="button" value="v"/>

Showing 1 to 1 of 1 entries

Previous **1** Next

Edit Terms of Use

Type

Version

Language

Title

Text (Html)

- ▶ 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



Users

Show entries

Search:

Email	First Name	Last Name	External Identity Provider	Actions
e.mustermann@dkfz-heidelberg.de	Erika	Mustermann	Local	
m.mustermann@dkfz-heidelberg.de	Max	Mustermann	Local	
s.muster@dkfz-heidelberg.de	Susanne	Muster	Local	

- Details
- Enable searchable
- Enable user
- Verify Email
- Edit user
- Enable/Disable authentication via client certificate
- Delete user

Showing 1 to 3 of 3 entries (filtered from 15 total entries)

- ▶ 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



Email

Password

[forgot password?](#)

[more login options](#)

Authentifizierung von Nutzern (DFN-AAI)





DEUTSCHES
KREBSFORSCHUNGSZENTRUM
IN DER HELMHOLTZ-GEMEINSCHAFT

[Über AAI](#)

Organisation auswählen

Um auf den Dienst **login.mitro.dkfz.de** zuzugreifen, wählen oder suchen Sie bitte die Organisation, der Sie angehören.

Wählen Sie die Organisation aus, der Sie angehören. ...

Wählen Sie die Organisation aus, der Sie angehören. ...

- Deutschland (DFN-AAI)**
- RWTH Aachen
- Charité - Universitätsmedizin Berlin
- Technische Universität Darmstadt
- Universität Duisburg-Essen
- Universität Erlangen-Nürnberg
- Universität Göttingen**
- Universität Greifswald
- Deutsches Krebsforschungszentrum Heidelberg
- Medizinische Hochschule Hannover
- Universität Leipzig
- Universität Mainz
- Helmholtz-Zentrum München
- Ludwig-Maximilians-Universität München (LMU)
- Technische Universität München (TUM)
- Universität Würzburg
- Funktionsprüfung**
- Humboldt-Universität zu Berlin
- Universität Bonn

Authentifizierung von Nutzern (DFN-AAI)



Georg-August-Universität Göttingen
Shibboleth Identity Provider

Single-Sign-On

For Students and Employees

Email:

Password:

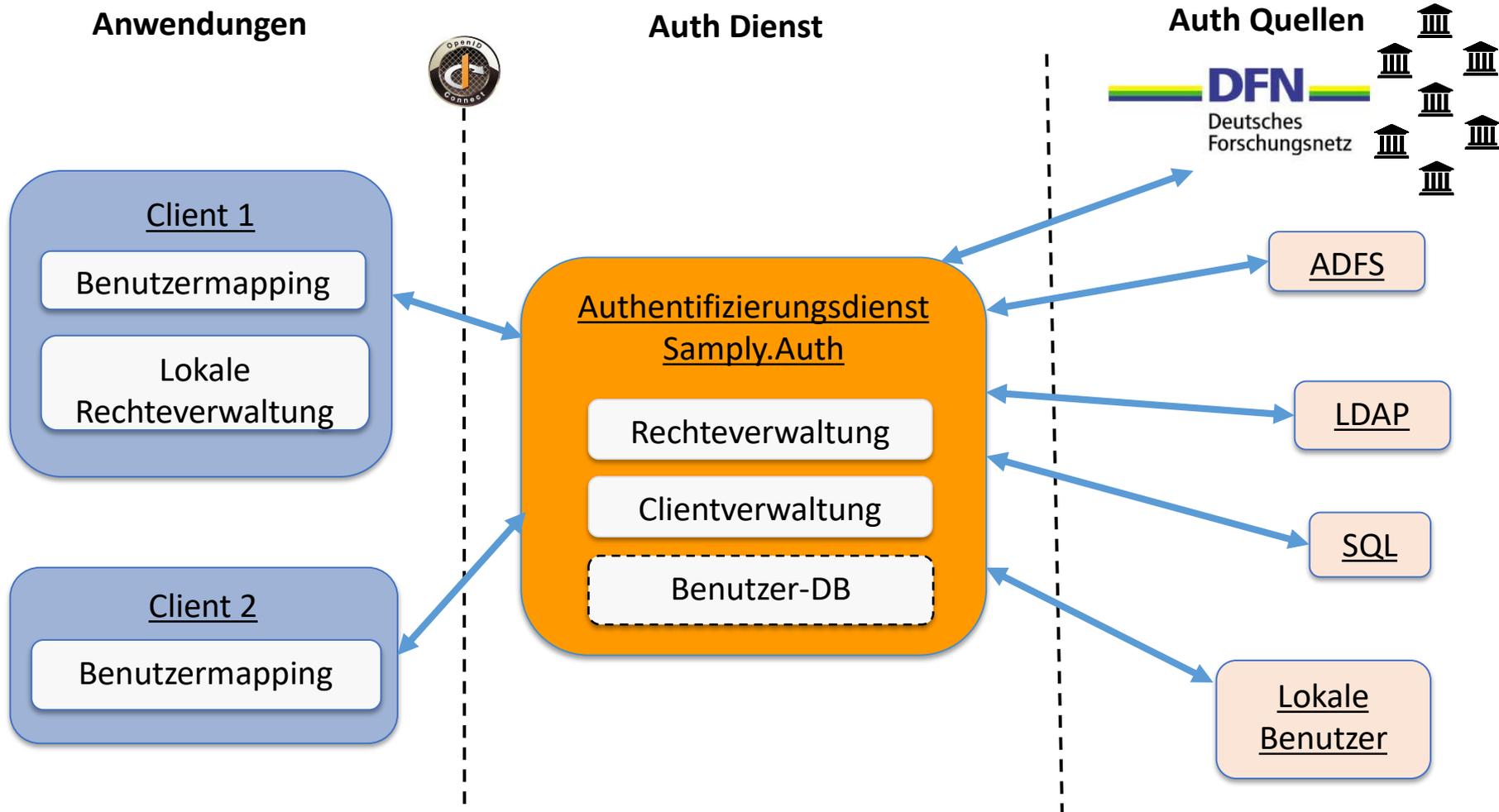
Log in to "Deutsches Krebsforschungszentrum: Medizinische Informatik in der Translationalen Onkologie".

default
Internetdienste der Abteilung Medizinische Informatik in der Translationalen Onkologie am Deutschen Krebsforschungszentrum (DKFZ), Heidelberg

For questions, feedback or reporting, please send an email to support@gwdg.de, yours

GWGD
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Authentifizierung von Nutzern: Implementierung



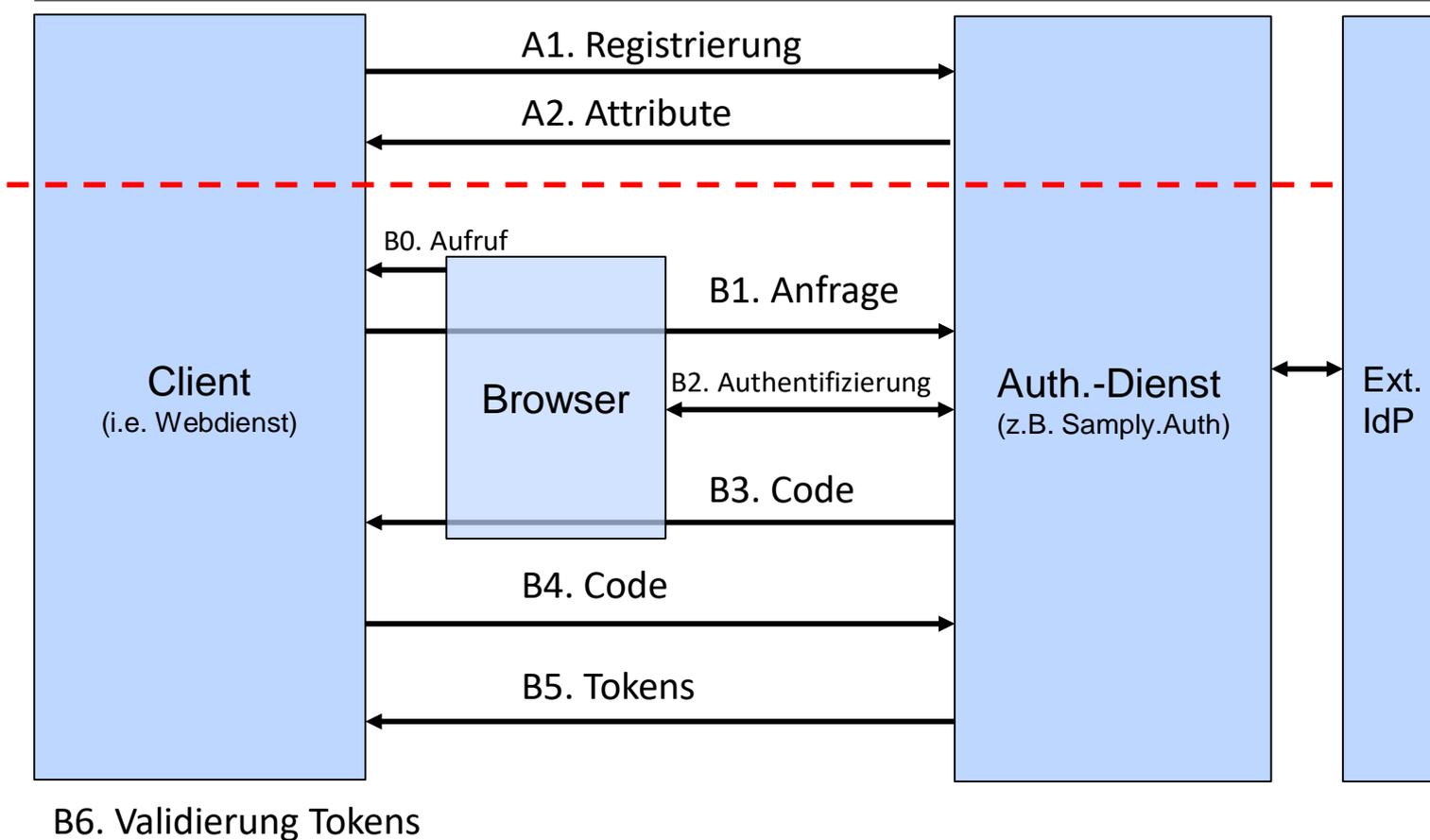
Externe Identity Provider

- ▶ **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

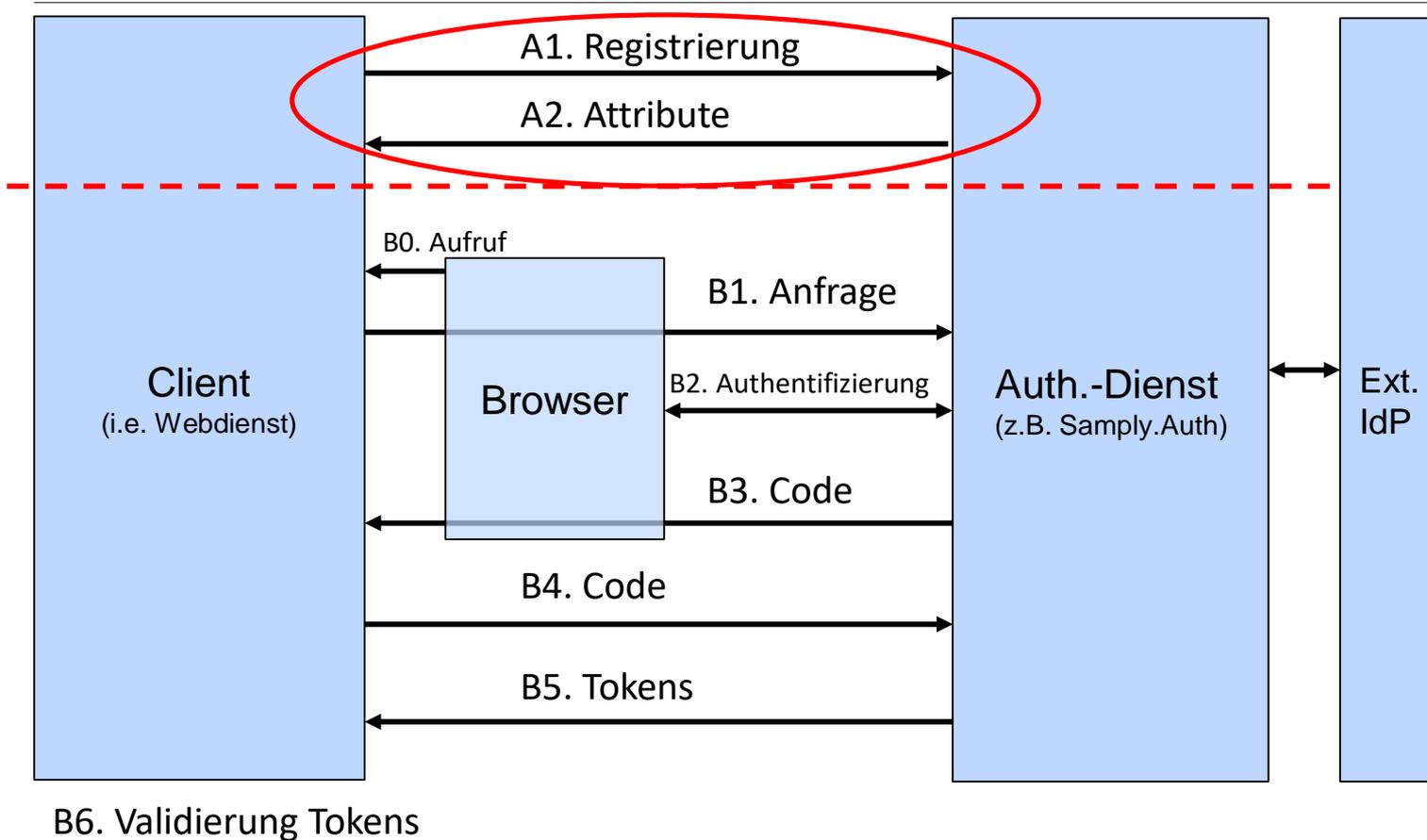
- ▶ Docker Container für Samply.Auth (bald verfügbar):
<https://bitbucket.org/medicalinformatics/samply.auth.webapp.docker/>
- ▶ Docker Konfigurationsdatei (samply.auth.config):
 - ▶ Konfigurationen für Datenbank, Netzwerk, Zugriff zur Admin-Oberfläche und Anbindung an DFN-AAI
- ▶ Kann sowohl für Samply.Auth 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



Beispiel-Ablauf anhand Samply.Auth

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

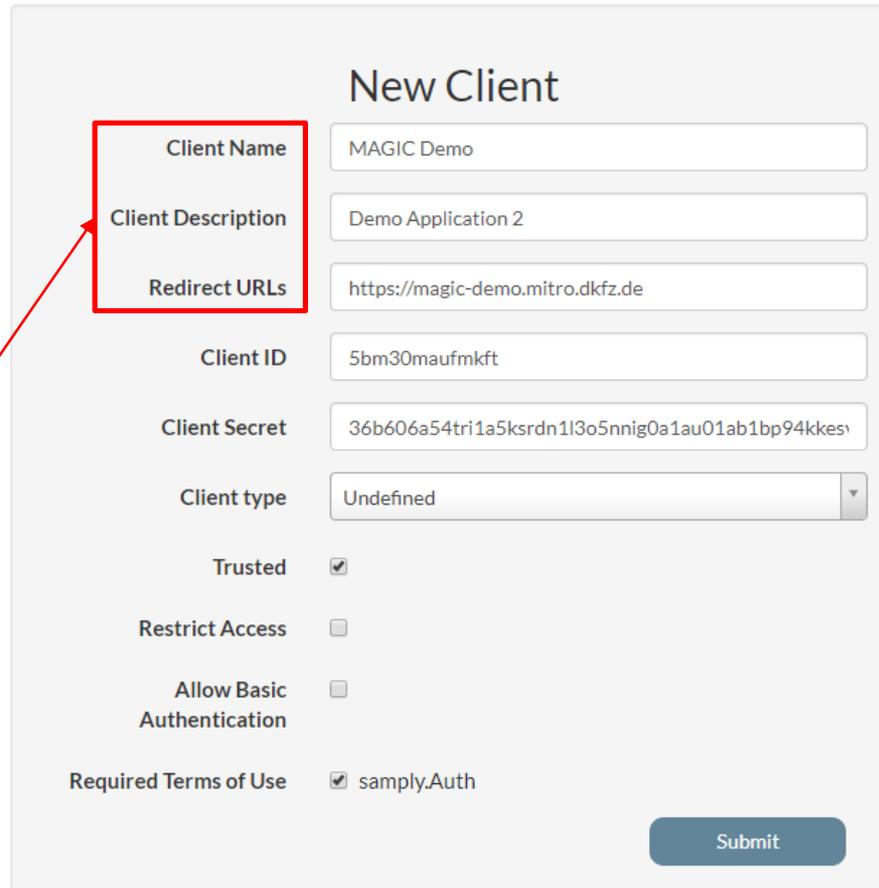
New Client

Client Name	<input type="text" value="MAGIC Demo"/>
Client Description	<input type="text" value="Demo Application 2"/>
Redirect URLs	<input type="text" value="https://magic-demo.mitro.dkfz.de"/>
Client ID	<input type="text" value="5bm30maufmkft"/>
Client Secret	<input type="text" value="36b606a54tri1a5ksrdn1l3o5nnig0a1au01ab1bp94kkesv"/>
Client type	<input type="text" value="Undefined"/>
Trusted	<input checked="" type="checkbox"/>
Restrict Access	<input type="checkbox"/>
Allow Basic Authentication	<input type="checkbox"/>
Required Terms of Use	<input checked="" type="checkbox"/> samply.Auth

Beispiel-Ablauf anhand Samply.Auth

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

Notwendige Eingaben für Registrierung eines Clients



New Client

Client Name: MAGIC Demo

Client Description: Demo Application 2

Redirect URLs: https://magic-demo.mitro.dkfz.de

Client ID: 5bm30maufmkft

Client Secret: 36b606a54tri1a5ksrdn1l3o5nnig0a1au01ab1bp94kkesv

Client type: Undefined

Trusted:

Restrict Access:

Allow Basic Authentication:

Required Terms of Use: samply.Auth

Submit

Beispiel-Ablauf anhand Samply.Auth

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

New Client

Client Name	<input type="text" value="MAGIC Demo"/>
Client Description	<input type="text" value="Demo Application 2"/>
Redirect URLs	<input type="text" value="https://magic-demo.mitro.dkfz.de"/>
Client ID	<input type="text" value="5bm30maufmkft"/>
Client Secret	<input type="text" value="36b606a54tri1a5ksrdn1l3o5nnig0a1au01ab1bp94kkesv"/>
Client type	<input type="text" value="Undefined"/>
Trusted	<input checked="" type="checkbox"/>
Restrict Access	<input type="checkbox"/>
Allow Basic Authentication	<input type="checkbox"/>
Required Terms of Use	<input checked="" type="checkbox"/> samply.Auth

URLs für die Validierung der redirect URLs

Beispiel-Ablauf anhand Ssamply.Auth

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

New Client

Client Name	<input type="text" value="MAGIC Demo"/>
Client Description	<input type="text" value="Demo Application 2"/>
Redirect URLs	<input type="text" value="https://magic-demo.mitro.dkfz.de"/>
Client ID	<input type="text" value="5bm30maufmkft"/>
Client Secret	<input type="text" value="36b606a54tri1a5ksrdn113o5nnig0a1au01ab1bp94kkesv"/>
Client type	<input type="text" value="Undefined"/>
Trusted	<input checked="" type="checkbox"/>
Restrict Access	<input type="checkbox"/>
Allow Basic Authentication	<input type="checkbox"/>
Required Terms of Use	<input checked="" type="checkbox"/> <small>samply.Auth</small>

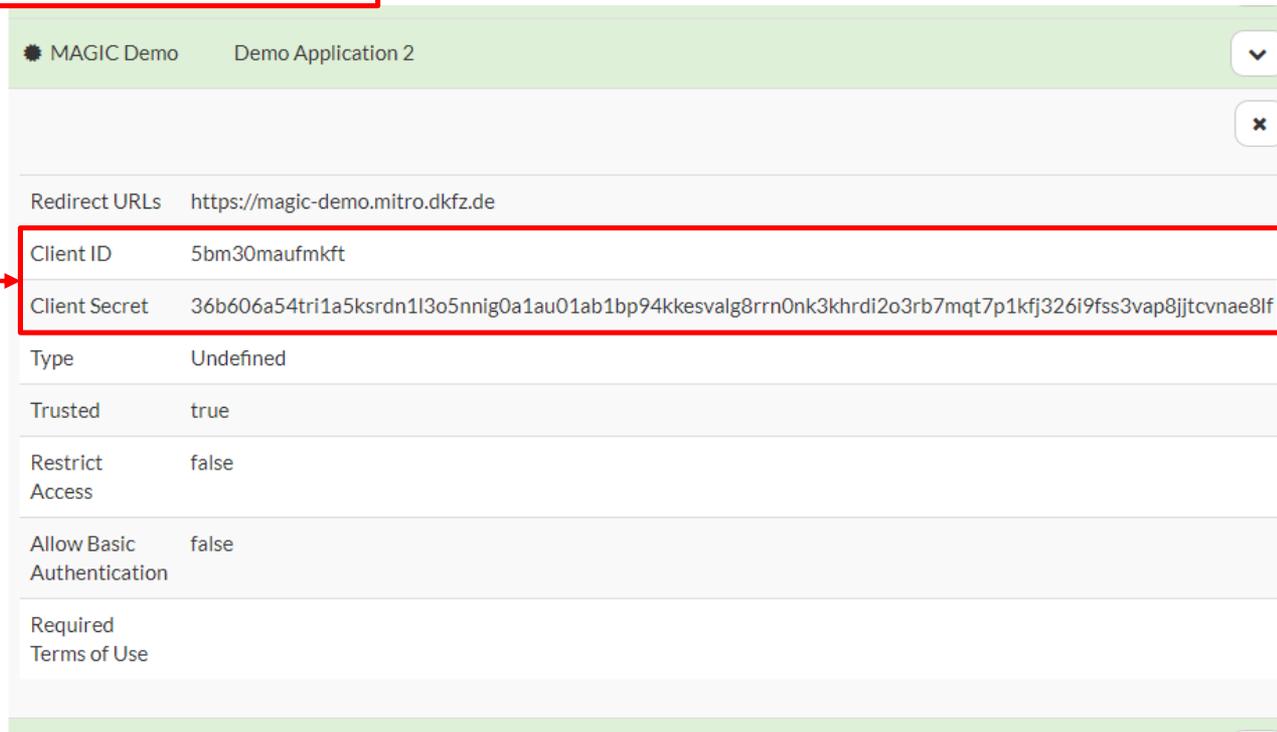
True:
Zugriff nur für
berechtigte
Benutzer
False:
Zugriff für alle



Beispiel-Ablauf anhand Samplly.Auth

A2. Antwort von Auth-Admin:

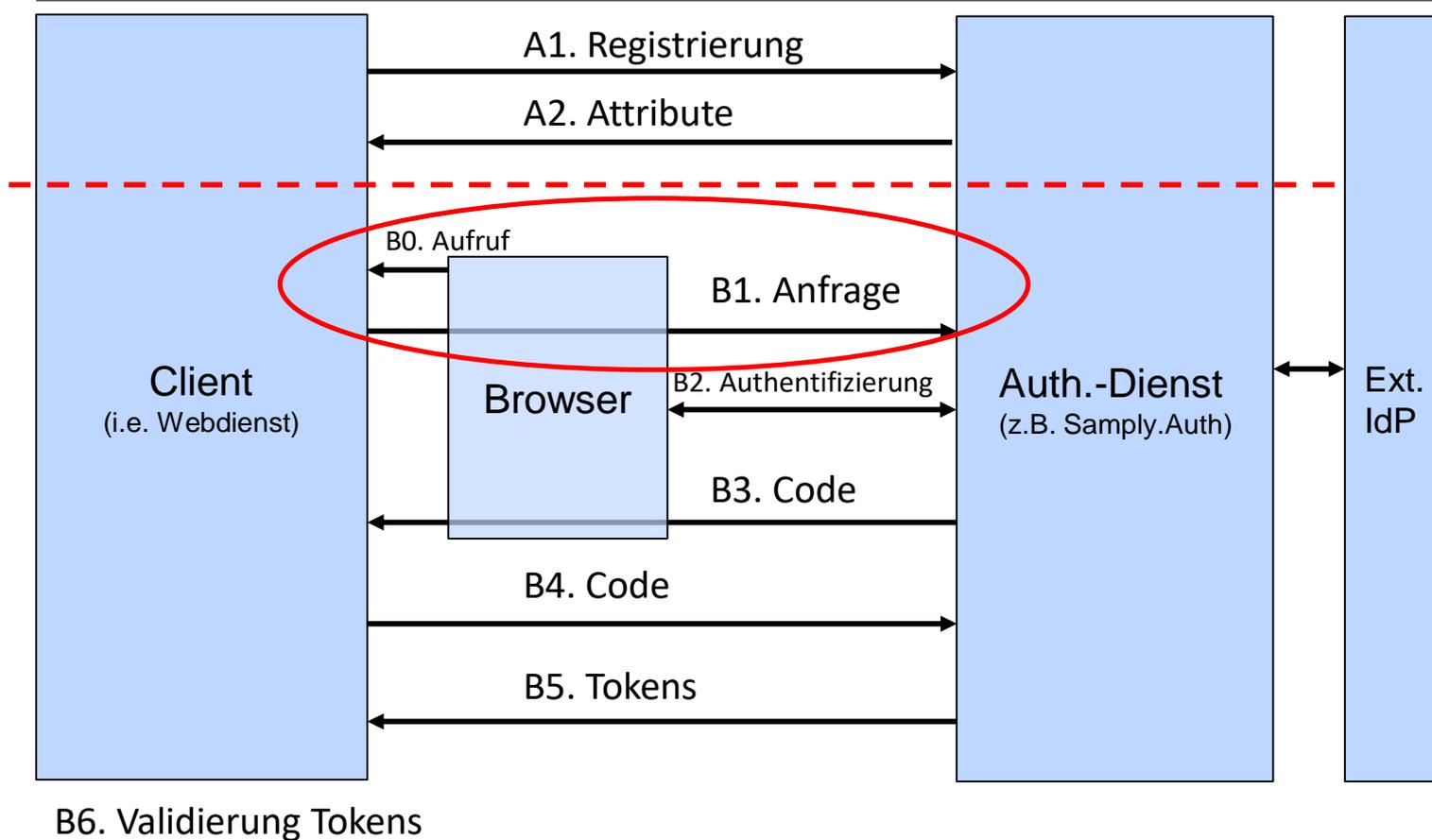
Client ID, Client Secret, Auth Base URL



MAGIC Demo Demo Application 2	
Redirect URLs	https://magic-demo.mitro.dkfz.de
Client ID	5bm30maufmkft
Client Secret	36b606a54tri1a5ksrdn1l3o5nnig0a1au01ab1bp94kkesvalg8rrn0nk3khrdi2o3rb7mqt7p1kfj326i9fss3vap8jjtcvnae8lf
Type	Undefined
Trusted	true
Restrict Access	false
Allow Basic Authentication	false
Required Terms of Use	

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

Anbindung eines Webdienstes an Auth Dienst



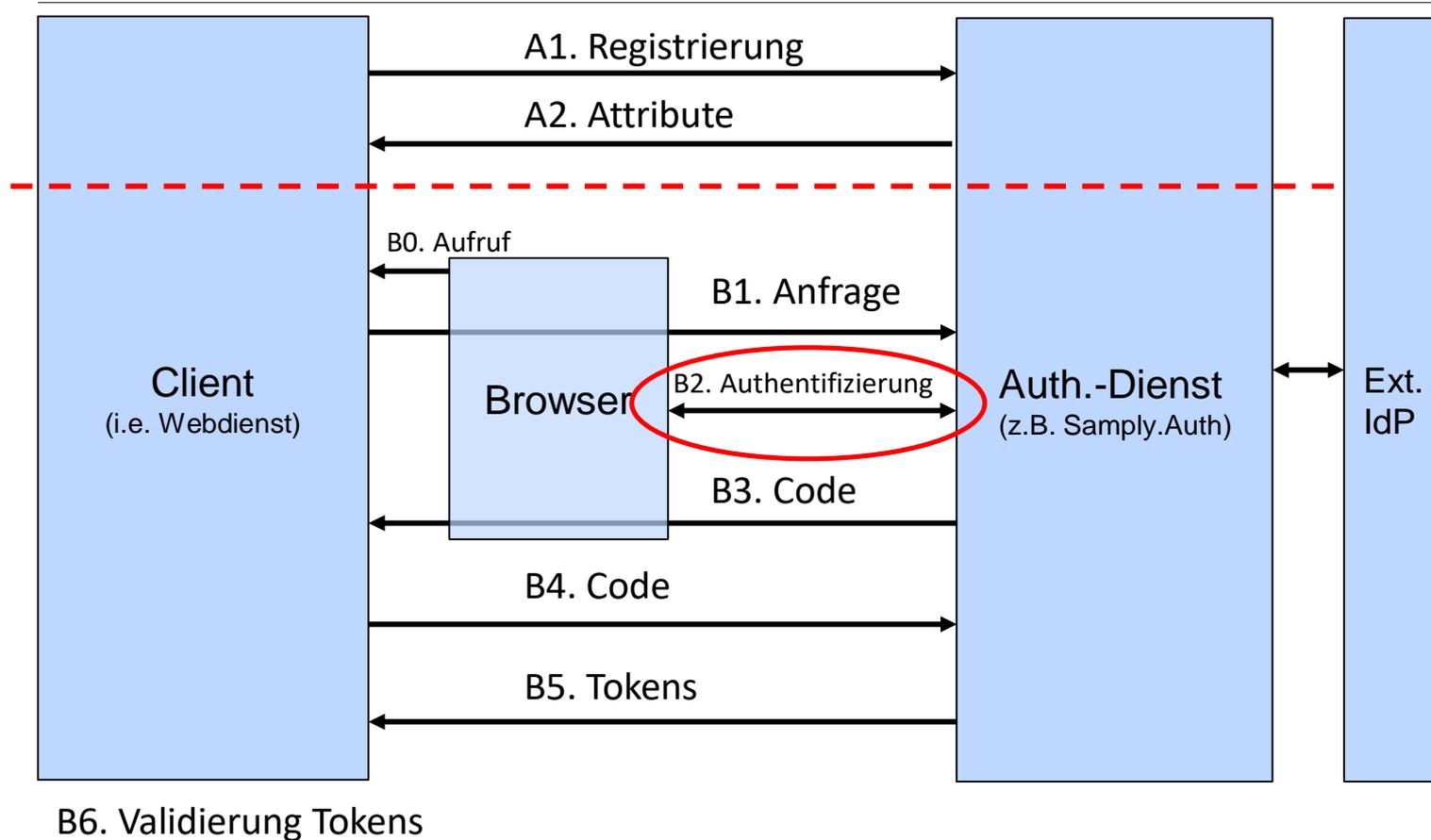
Beispiel-Ablauf anhand Samply.Auth

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

B1. Client redirected Browser an Samply.Auth

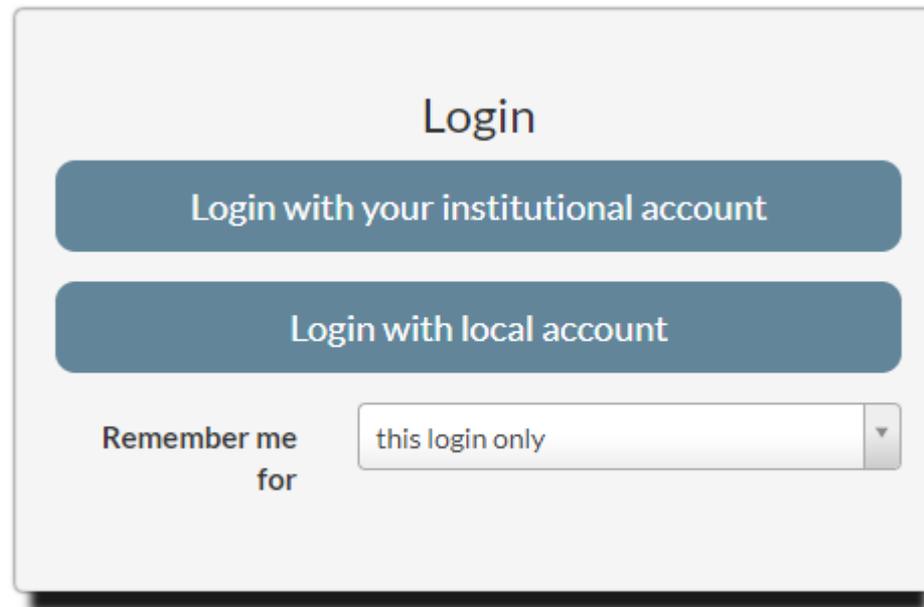
```
https://login.verbis.dkfz.de/auth/grant.xhtml  
    ?client_id=5bm30maufmkft  
    &redirect_uri=https%3A%2F%2Fmagic-demo.mitro.dkfz.de  
    &scope=openid  
    &state=af0ifjsldkj
```

Anbindung eines Webdienstes an Auth Dienst



Beispiel-Ablauf anhand Samply.Auth

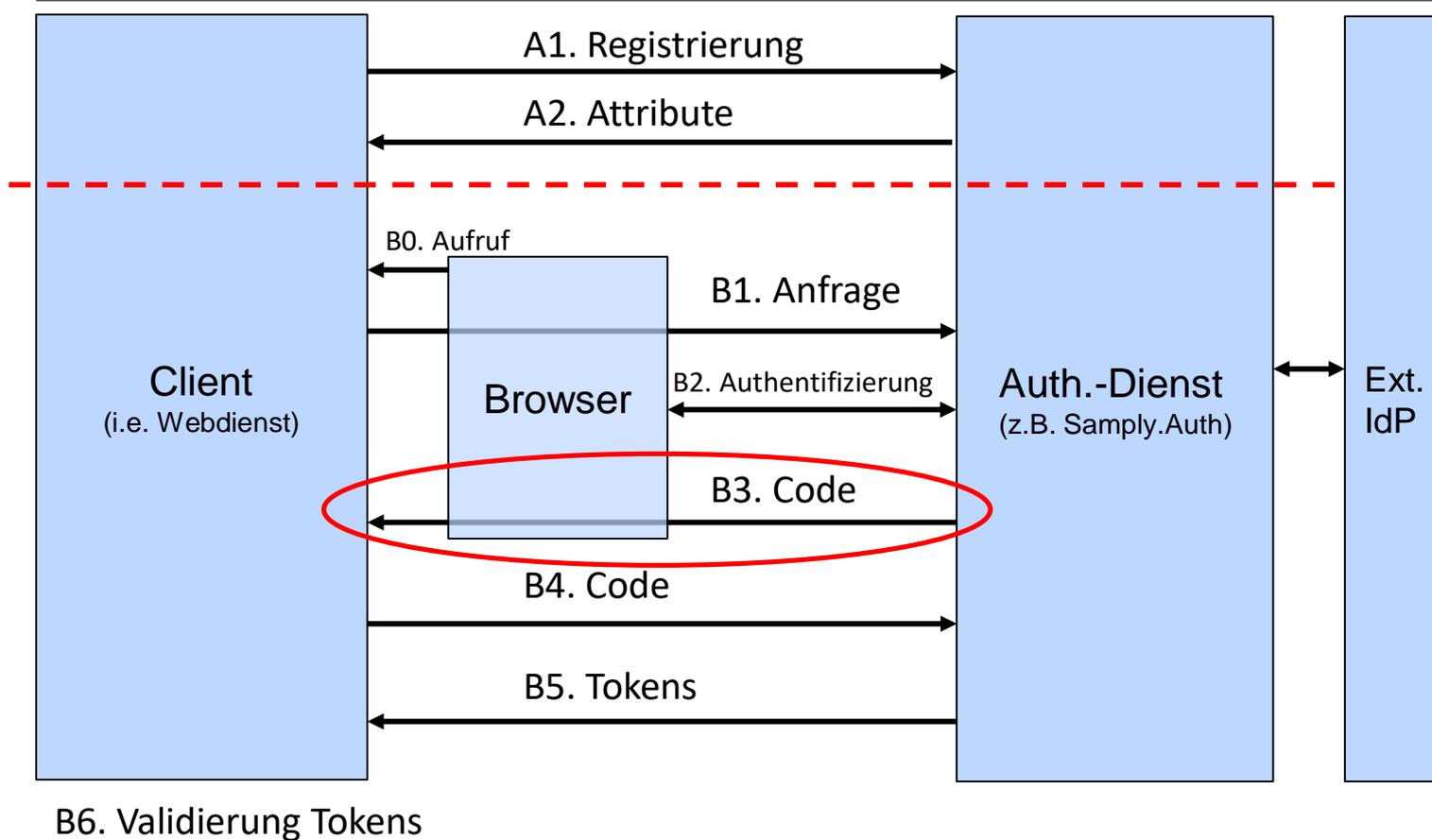
B2. (Samply.Auth authentifiziert Nutzer gegen einen IdP)



The image shows a login form with the following elements:

- Title:** Login
- Buttons:** Two large blue buttons: "Login with your institutional account" and "Login with local account".
- Remember me section:** The text "Remember me for" is followed by a dropdown menu.
- Dropdown menu:** The selected option is "this login only".

Anbindung eines Webdienstes an Auth Dienst



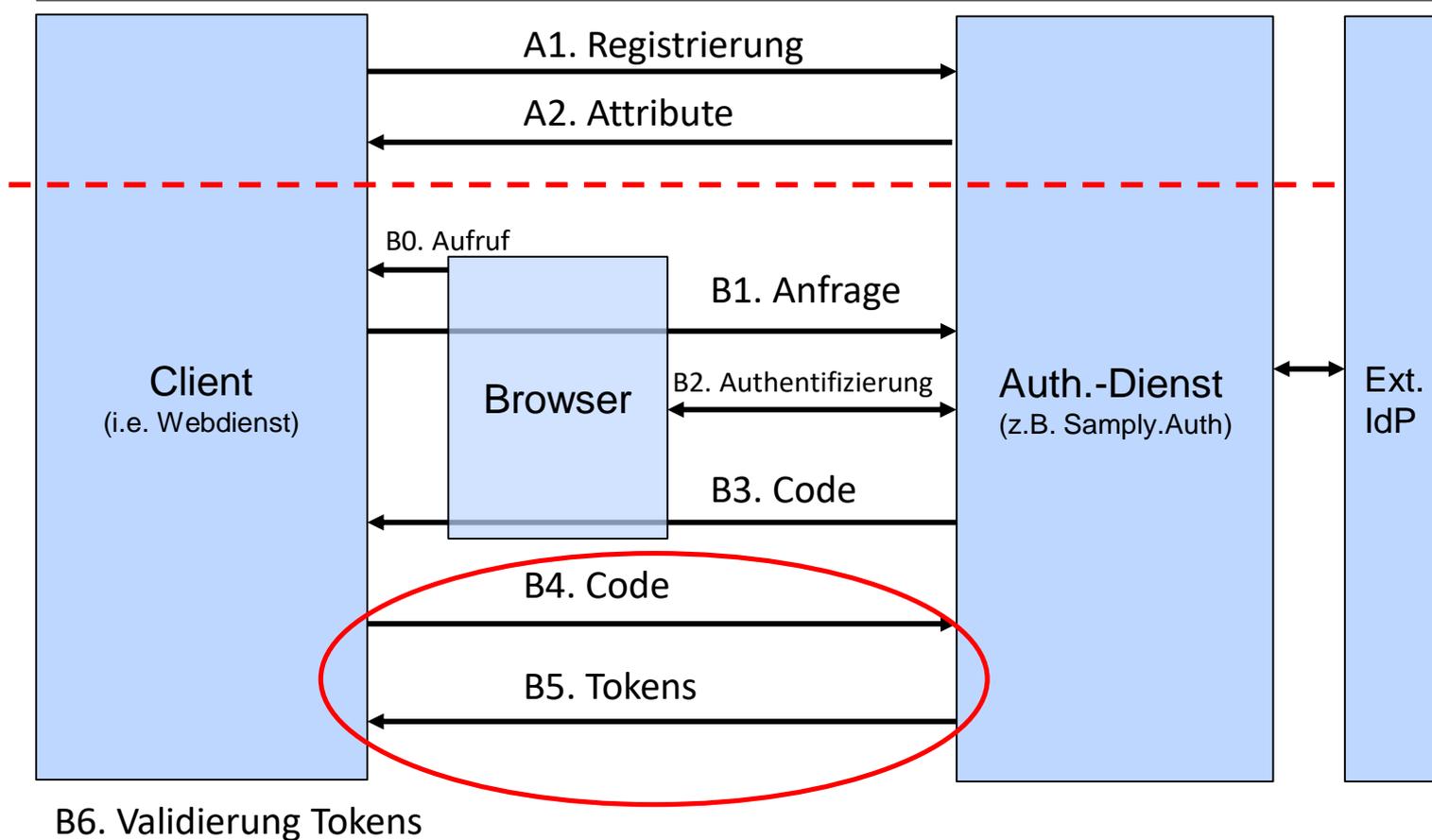
Beispiel-Ablauf anhand Samply.Auth



B3. Samply.Auth redirected Browser zurück zu Client:

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

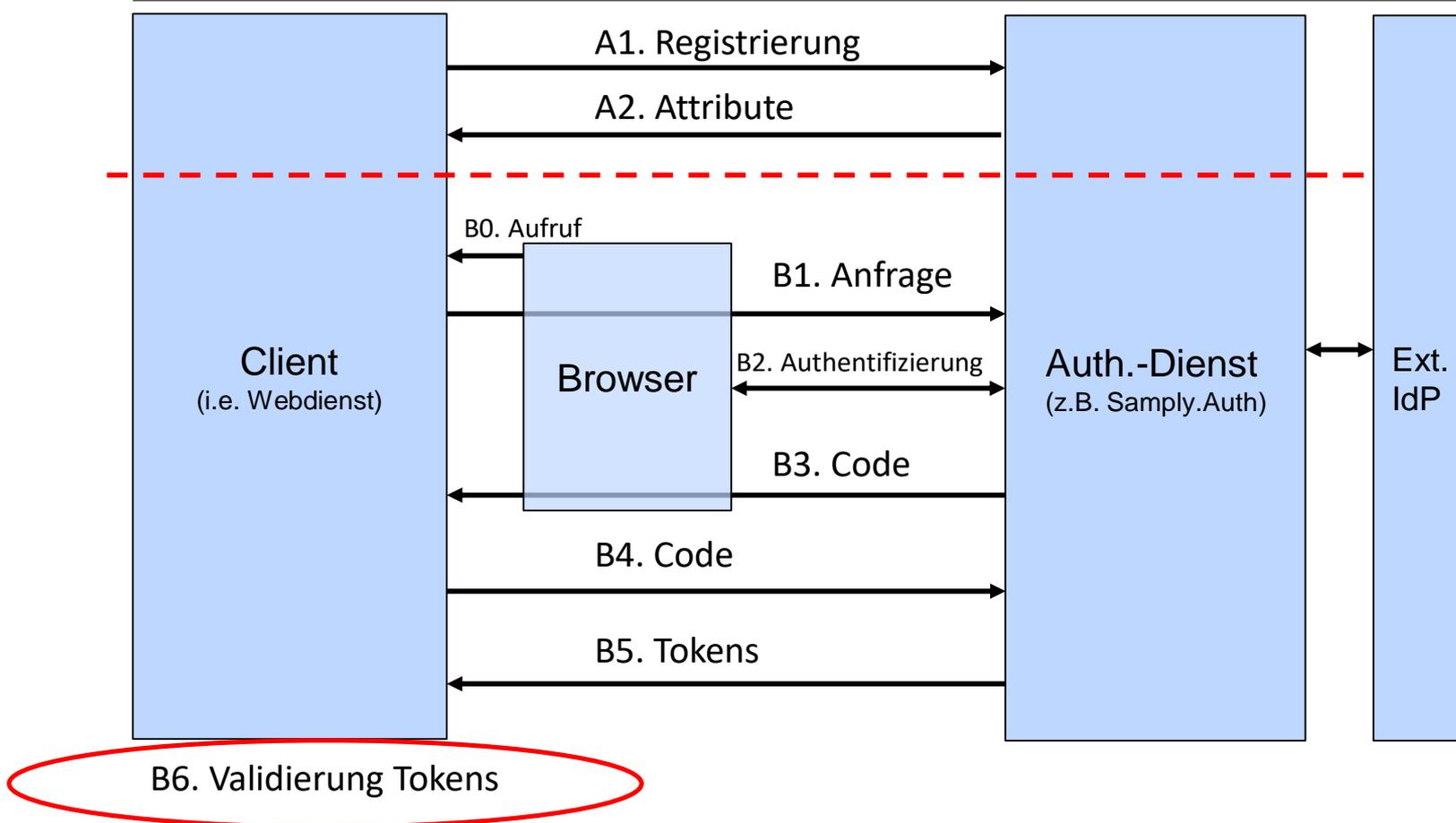
POST <https://login.verbis.dkfz.de/auth/oauth2/token>

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

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

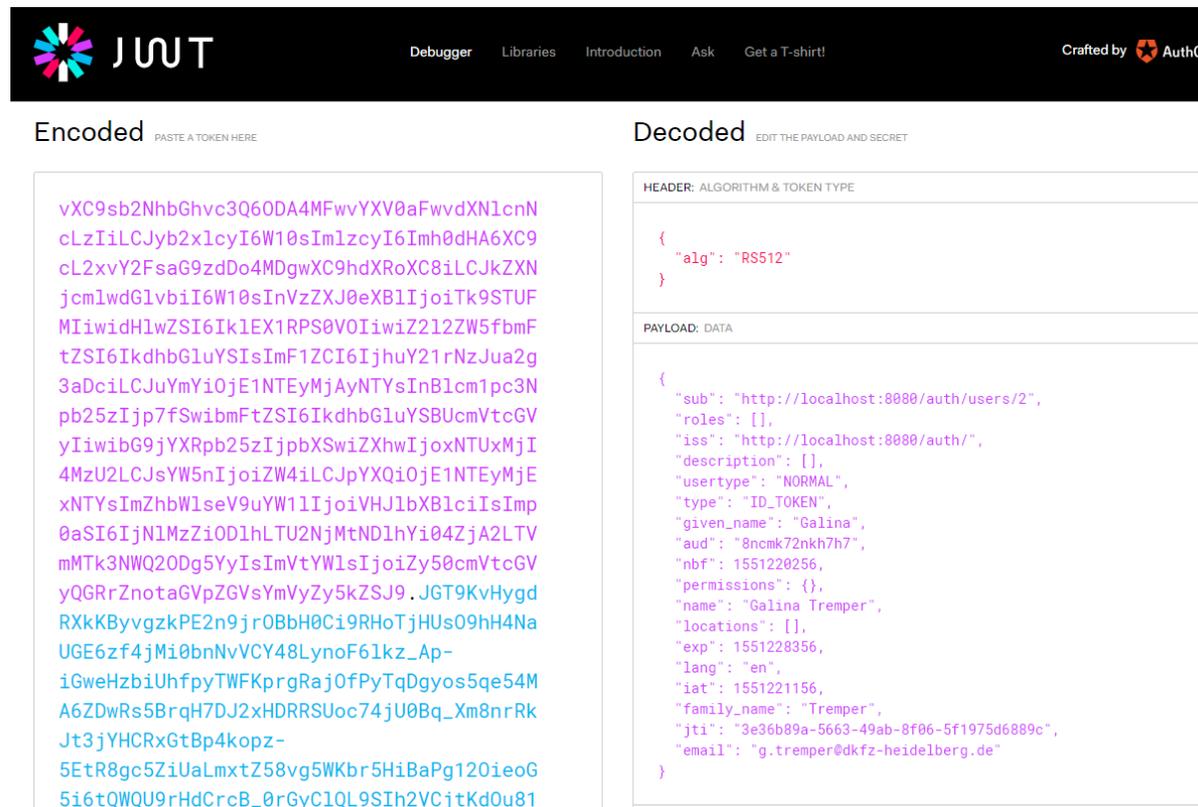
```
{  
  "access_token" : "eyJhbG[...]miKeNDI",  
  "id_token" : "eyJhbG[...]iG6C2I",  
  "refresh_token" : "36b606a[...]dxXOULg ",  
  "token_type" : "Bearer",  
  "expires_in" : 7200  
}
```

Anbindung eines Webdienstes an Auth Dienst



Beispiel-Ablauf anhand Samply.Auth

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



The screenshot shows the JWT.io interface. On the left, under 'Encoded', a long base64-encoded token is pasted. On the right, under 'Decoded', the token's structure is shown, including the header and the decoded payload.

Encoded PASTE A TOKEN HERE

```
vXC9sb2NhbGhvc3Q6ODA4MFwvYXV0aFwvdXNlcnN
cLzIiLCJyb2xlcYI6W10sImIzcyI6Imh0dHA6XC9
cL2xvY2FsaG9zdDo4MDgwXC9hdXRoXC8iLCJkZXN
jcmldGlvbiI6W10sInVzZXJ0eXB1IjoITk9STUF
MIiwidHlwZSI6IklEX1RPS0V0IiwiZ212ZW5fbmF
tZSI6IkdhbGluYSIsImF1ZCI6IjhuY21rNzJua2g
3aDciLCJmYmY0IjE1NTEyMjAyNTYsInBlcm1pc3N
pb25zIjpw7fSwibmFtZSI6IkdhbGluYSBUcmVtcGV
yIiwibG9jYXRpb25zIjpbXSwiZXhwIjoxNTUxMjI
4MzU2LzY5W5nIjoITk9STUF0eXB1IjoITk9STUF
xNTYsImZhbnVseV9uYmY1IiwiVHJlbnB1ciIsImp
0aSI6IjNlMzZiOD1hLTU2NjMtND1hYi04ZjA2LTV
mMTk3NWQ2ODg5YyIsImVtYWlsIjoITk9STUF0eXB1IjoITk9STUF
yQGRrZnotaGVpZGVsYmVzYy5kZSJ9.JGT9KvHygd
RXkKByvgzkPE2n9jr0BbH0Ci9RH0TjHUs09hH4Na
UGE6zf4jMi0bnNvVCY48LynoF6lkz_Ap-
iGweHzbiUhfpyTWFkprgRaj0fPyTqDgyos5qe54M
A6ZDwRs5BrqH7DJ2xHRRSUoc74jU0Bq_Xm8nrRk
Jt3jYHCRxGtBp4kopz-
5EtR8gc5ZiUaLmxtZ58vg5WKbr5HiBaPg120ieoG
5i6tQWQU9rHdCrcB_0rGyC1QL9SIh2VCjtKd0u81
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS512"
}
```

PAYLOAD: DATA

```
{
  "sub": "http://localhost:8080/auth/users/2",
  "roles": [],
  "iss": "http://localhost:8080/auth/",
  "description": [],
  "usertype": "NORMAL",
  "type": "ID_TOKEN",
  "given_name": "Galina",
  "aud": "8ncmk72nkh7h7",
  "nbf": 1551220256,
  "permissions": {},
  "name": "Galina Tremper",
  "locations": [],
  "exp": 1551228356,
  "lang": "en",
  "iat": 1551221156,
  "family_name": "Tremper",
  "jti": "3e36b89a-5663-49ab-8f06-5f1975d6889c",
  "email": "g.tremper@dkfz-heidelberg.de"
}
```

jwt.io

Beispiel-Ablauf anhand Samply.Auth



Access Token

The screenshot shows the jwt.io interface with the following details:

- ALGORITHM: RS512
- Encoded token: `cLzIiLCJuYmYiOjE1NTEyMjAyNTYsInB1cm1pc3Npb25zIjp7fSwic2NvcGUiO1sib3BlbmlkI10sIm1zcyI6Imh0dHA6XC9cL2xvY2FsaG9zdDo4MDgwXC9hdXRoXC8iLCJzdGF0ZSI6InVuc3VwcG9ydGVkIiwidHlwZSI6IkFDQ0VTU19UT0tFTiIsImV4cCI6MTU1MTIyODM1NiwiawWF0IjoxNTUxMjIxMTU2LCJqdGkiOiJkZGM4NDBhOC0yYjVlLTR1NjMtYTc1Yi03MThiZTgxY2JkNjUiFQ.JLGwNXFHvHLJFpDMpXq50IuQWwL0cMHhXSPDBgfA7KsKsKymsUu-A6RyVx7AKpDImGAnoc0_32BPF4azDG6dg0D1K65yhWYn4Qe5ueTGM0Skz8eJoMuie-5QZdz7-gAlEoibC_0rgbofQ9dWFVPE6ZZGtNq3TfmHSJls_GZPlsFv4rj6y-uAK8P-eEssQiqMQyqHCc9KJX2g7Bxd1Zuz0G7Tgos-16SWHRFc6mW_suiywxalCLk7SD4bfmM2FeVED-7RVJ-36PEJk1Q1FBDfhdPbpqsuRgr7Ik34YCF715o-oc3fYbvr2111CzR9_A9jUDGMK_8WuR6Q89dRwGojs6PcOR3F0uaJjuqHkoPmzpCeqqfPz5fCoDuR6zs73WuoA87DqwOw1P-`
- Decoded payload (DATA):

```
{  "sub": "http://localhost:8080/auth/users/2",  "nbf": 1551220256,  "permissions": {},  "scope": [    "openid"  ],  "iss": "http://localhost:8080/auth/",  "state": "unsupported",  "type": "ACCESS_TOKEN",  "exp": 1551228356,  "iat": 1551221156,  "jti": "ddc840a8-2b5b-4e63-a75b-718be81cbd65"}
```
- Verify Signature: RSASHA512(base64UrlEncode(header) + "." + ...)

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/>

- ▶ Attribute für die erfolgreiche Anmeldung in Samplly.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))

The screenshot displays the Samplify Auth web interface. At the top, there are logos for DFN Deutsches and dkfz. DEUTSCHES KREBSFORSCHUNGSZENTRUM IN DER HELMHOLTZ-GEMEINSCHAFT. The main content area features a central box titled "Shibboleth Authentication Test" with three checked items: "Authenticated via Shibboleth", "Persistent ID", and "Identity Provider sends all requested attributes". Below this box, it states "The Authentication via Shibboleth works properly." At the bottom of the interface, there is a "Login" button and a checkbox labeled "Clear my attribute release consent".

- ▶ 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.

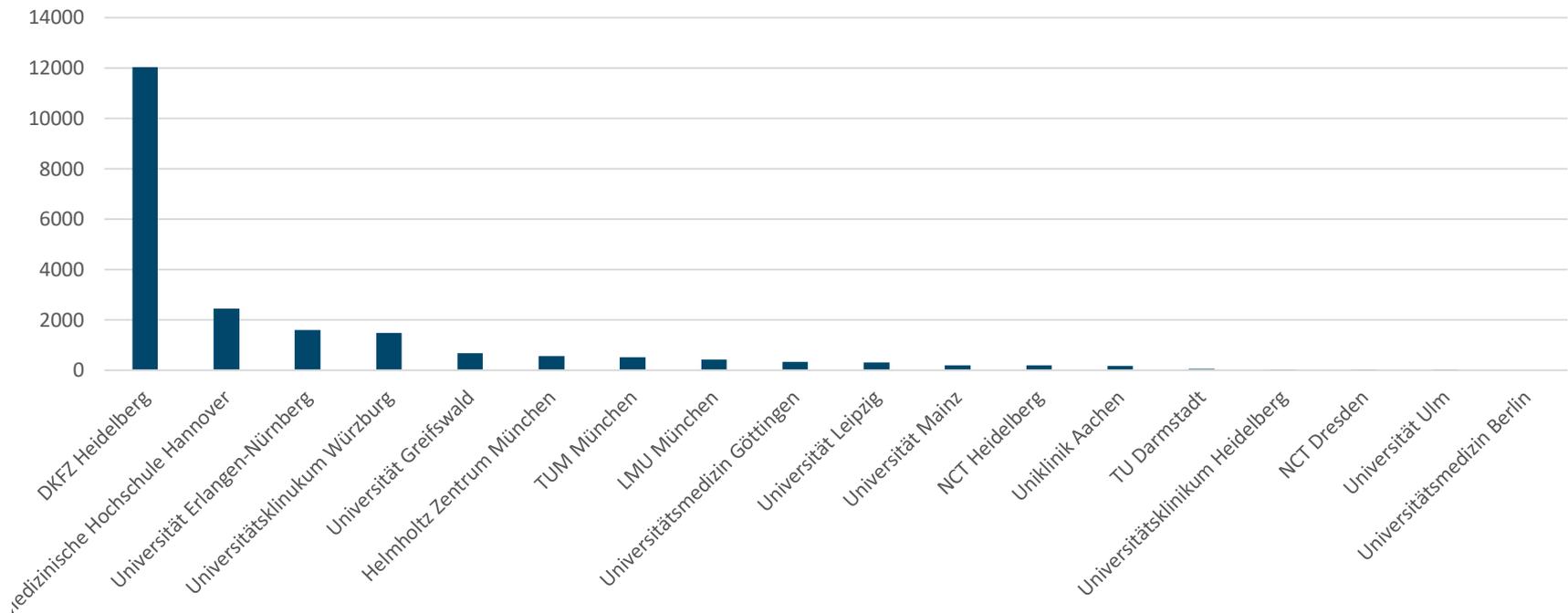
Mit freundlichem Gruß
<Name>

Praxisbeispiel föderierte Authentifizierung



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

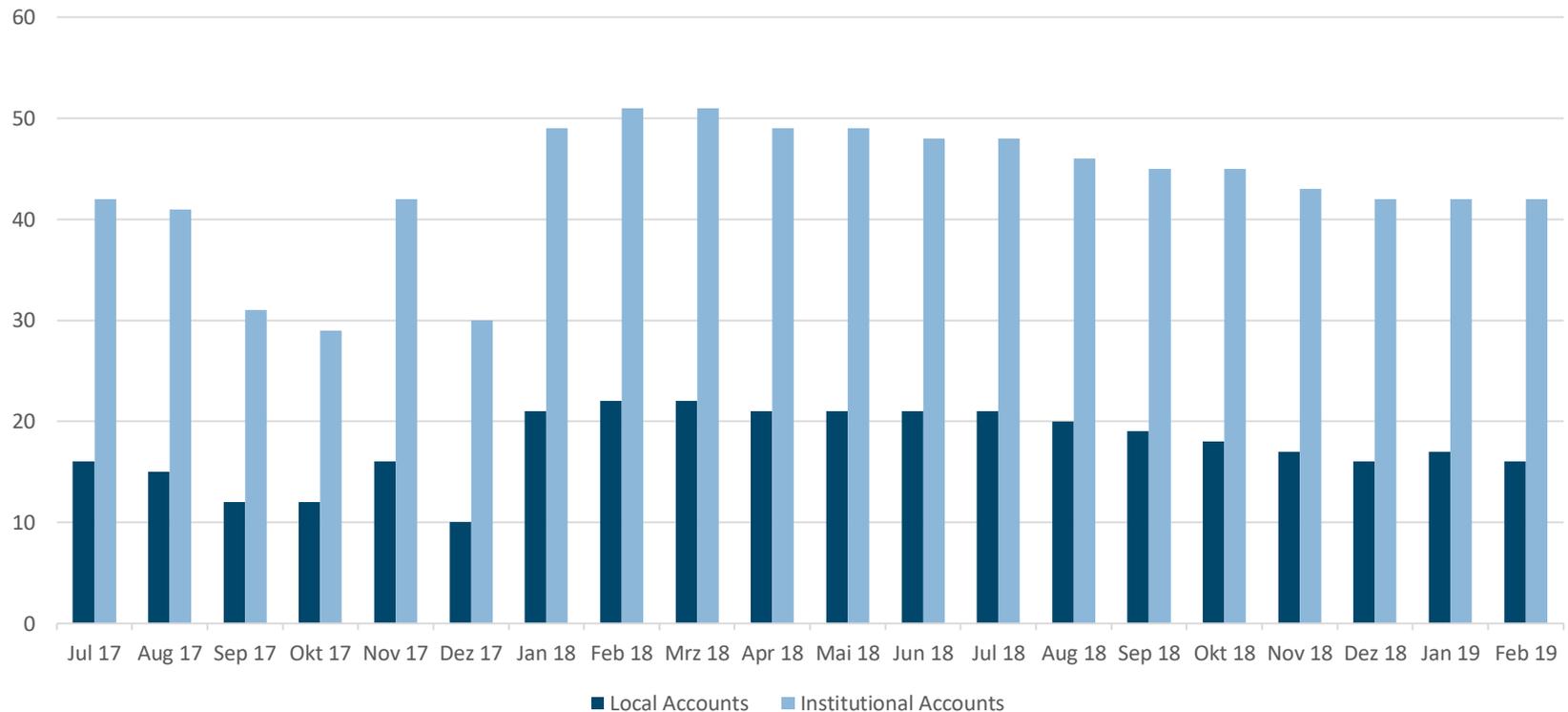
Anzahl Anmeldungen nach Einrichtungen



Praxisbeispiel föderierte Authentifizierung



Anzahl der Anmeldungen mit DFN-AAI und lokalen Accounts (durchschnittlich pro Tag)



Demo





Produkte Themen Projektplanung Über das Portal Mitmachen



Produkt > Software

Samply.Auth

Dieses Produkt wird entwickelt und bereitgestellt von Medizinische Informatik in der Translationalen Onkologie (MITRO), Deutsches Krebsforschungszentrum (DKFZ)



Kommentare

Software zur zentralen Authentifizierung und Autorisierung

Danke

