DARIAH AAI

ZKI AK Verzeichnisdienste
Heinrich-Heine-Universität Düsseldorf

Speaker: Peter Gietz
DAASI International

Date: 12.-13. September 2018

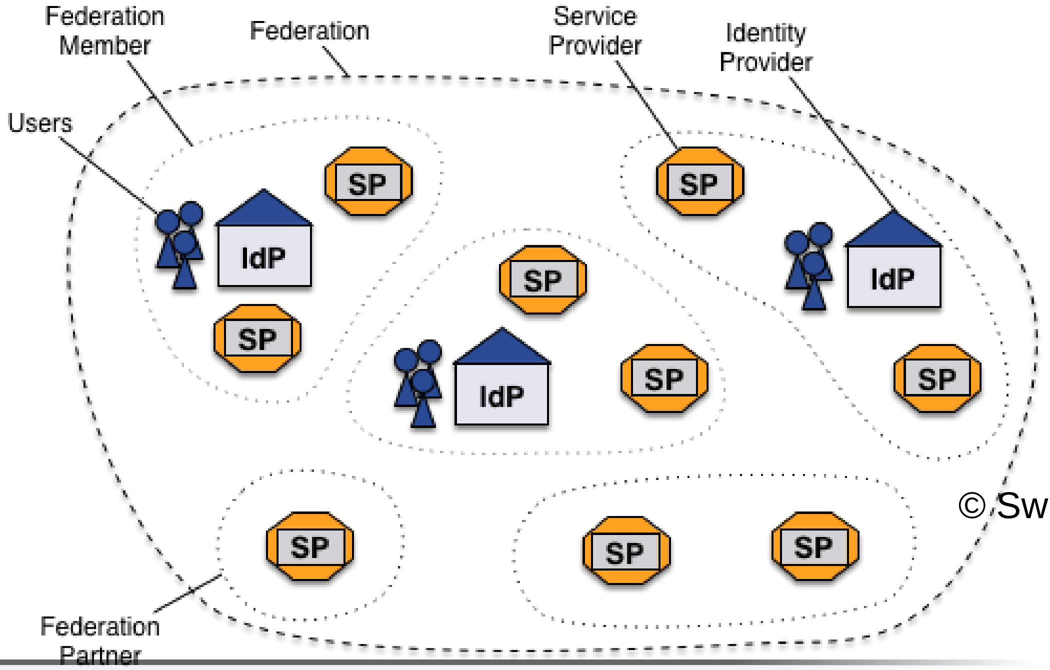
DARIAH-DE

AARC

Agenda

… and federations

- Federations as collection of organizations
- Federation operator as trusted third party
- Scalable way to allow SSO across organizational boundaries
- SAML Metadata to connect entities

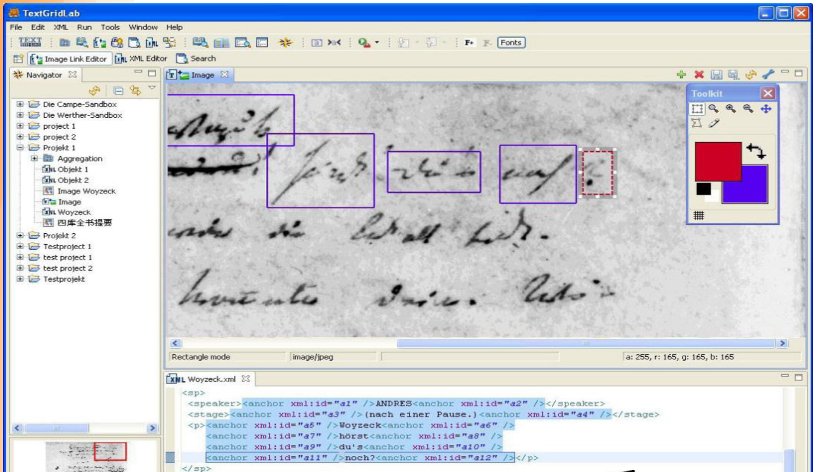


© Switch.ch

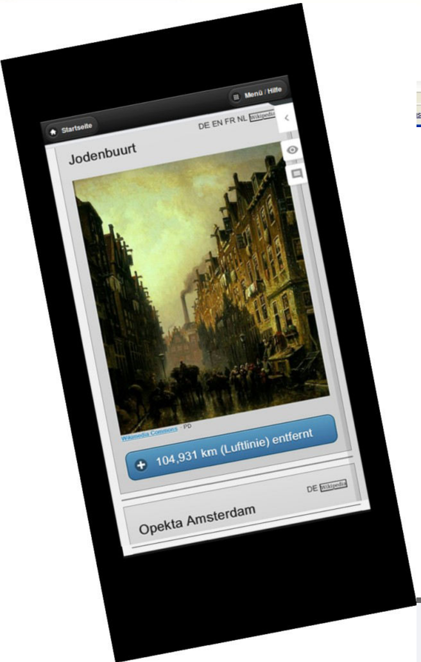
What is DARIAH

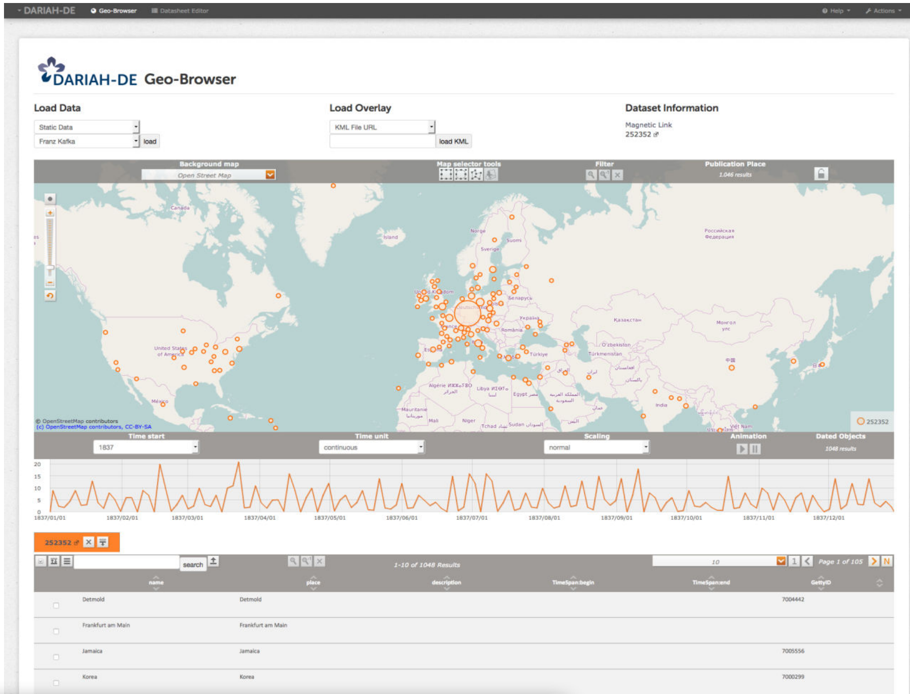
- DARIAH: Digital Research Infrastructure for the Arts and Humanities
- DARIAH is a pan-european infrastructure for arts and humanities scholars working with computational methods. It supports digital research as well as the teaching of digital research methods.
- One of the few ESFRI research infrastructures for the humanities (ERIC is in working since 2014)
- DARIAH’s mission is to develop, maintain and operate an infrastructure in support of ICT-based research practices Infrastructure is administration, software and storage services but also Curricula and Methodology
- Working with communities of practice: humanities scholars supporting their VREs

Virtual Research Environments in the humanities



```
<sp>
 <speaker><anchor xml:id="a1" />ANDRES<anchor xml:id="a2" /></speaker>
 <stage><anchor xml:id="a3" />(nach einer Pause.)<anchor xml:id="a4" /></stage>
 <p><anchor xml:id="a5" />Woyzeck<anchor xml:id="a6" />
    <anchor xml:id="a7" />hörst<anchor xml:id="a8" />
    <anchor xml:id="a9" />du's<anchor xml:id="a10" />
    <anchor xml:id="a11" />noch?<anchor xml:id="a12" /></p>
</sp>
<sp>
 <speaker>WOYZECK</speake
 <p>Still, Alles still, a
</sp>
<sp>
 <speaker>ANDRES</speaker
 <p>Hörst du? Sie trommel
```





Load Data

Static Data

Franz Kafka — load

Load Overlay

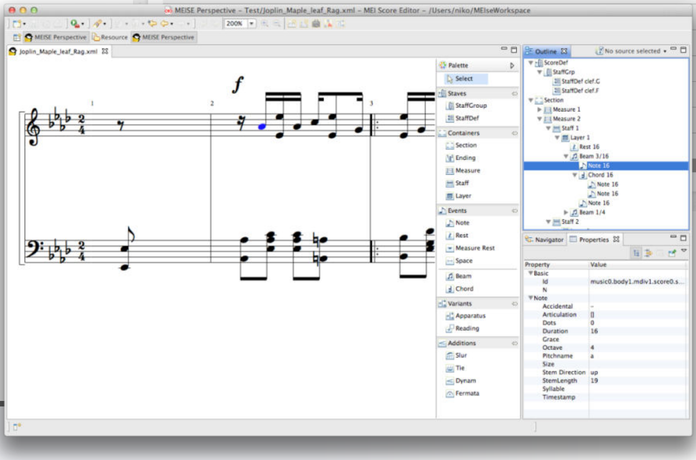
KML File URL — load KML

Dataset Information

Magnetic Link 252352

Time start: 1837 · Time unit: continuous · Scaling: normal

name	place	description	TimeSpan:begin	TimeSpan:end	GettyID
Detmold	Detmold				7004442
Frankfurt am Main	Frankfurt am Main				
Jamaica	Jamaica				7005556
Korea	Korea				7000299

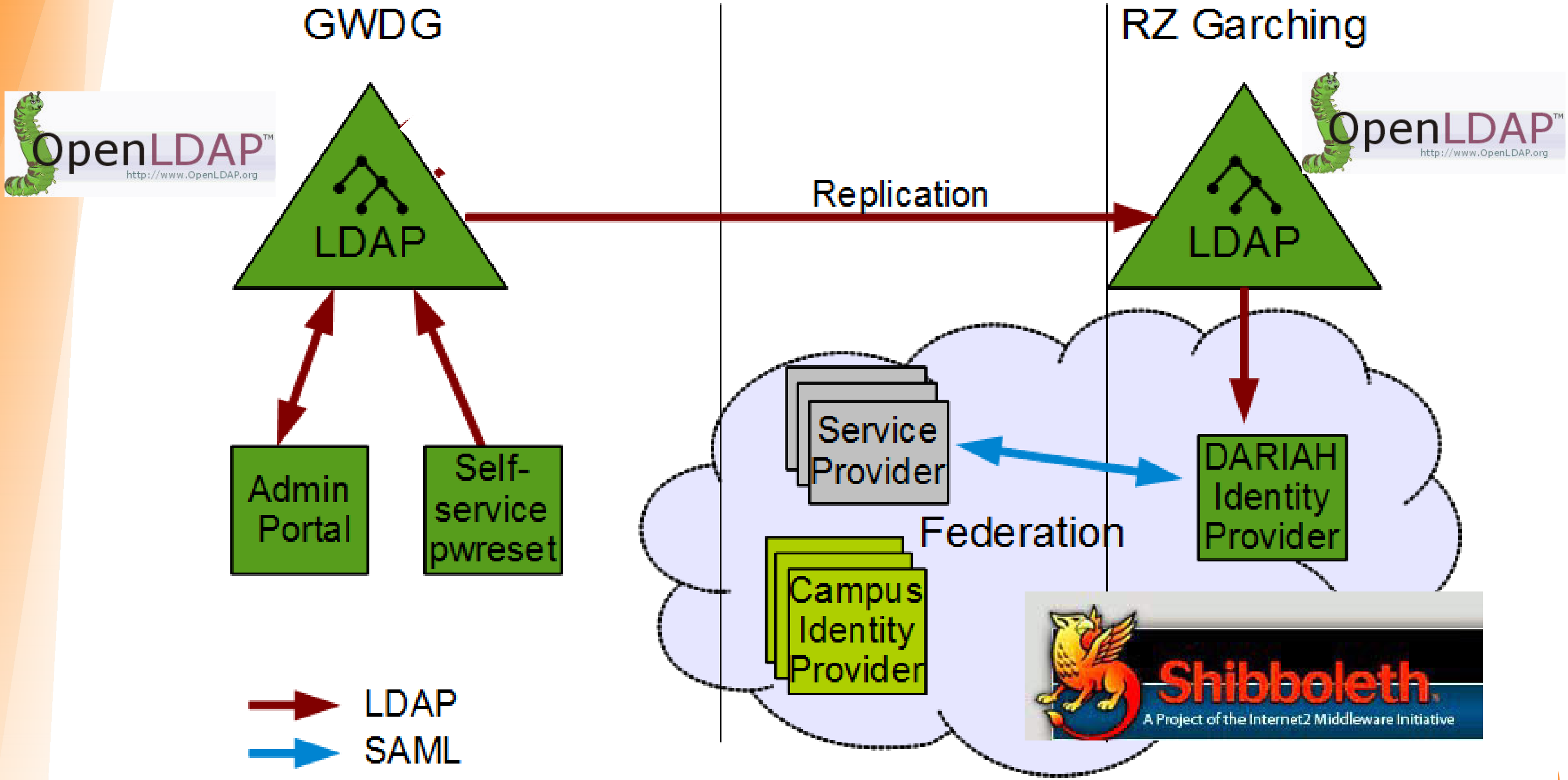


Property	Value
Basic	
Id	music0.body1.mdiv1.score0.s...
N	
Note	
Accidental	-
Articulation	[]
Dots	0
Duration	16
Grace	
Octave	4
Pitchname	a
Size	
Stem Direction	up
StemLength	19
Syllable	
Timestamp	

DARIAH AAI

- Since 2006 DARIAH-DE runs a productive AAI that allows researcher around the world to authenticate with either their home institution account or with a dedicated DARIAH account, while benefiting from a Single Sign-On experience and fine-grained authorization mechanisms. To widen the usage of this infrastructure the DARIAH-EU WG FIM4D invites and helps all DARIAH members to integrate their services.

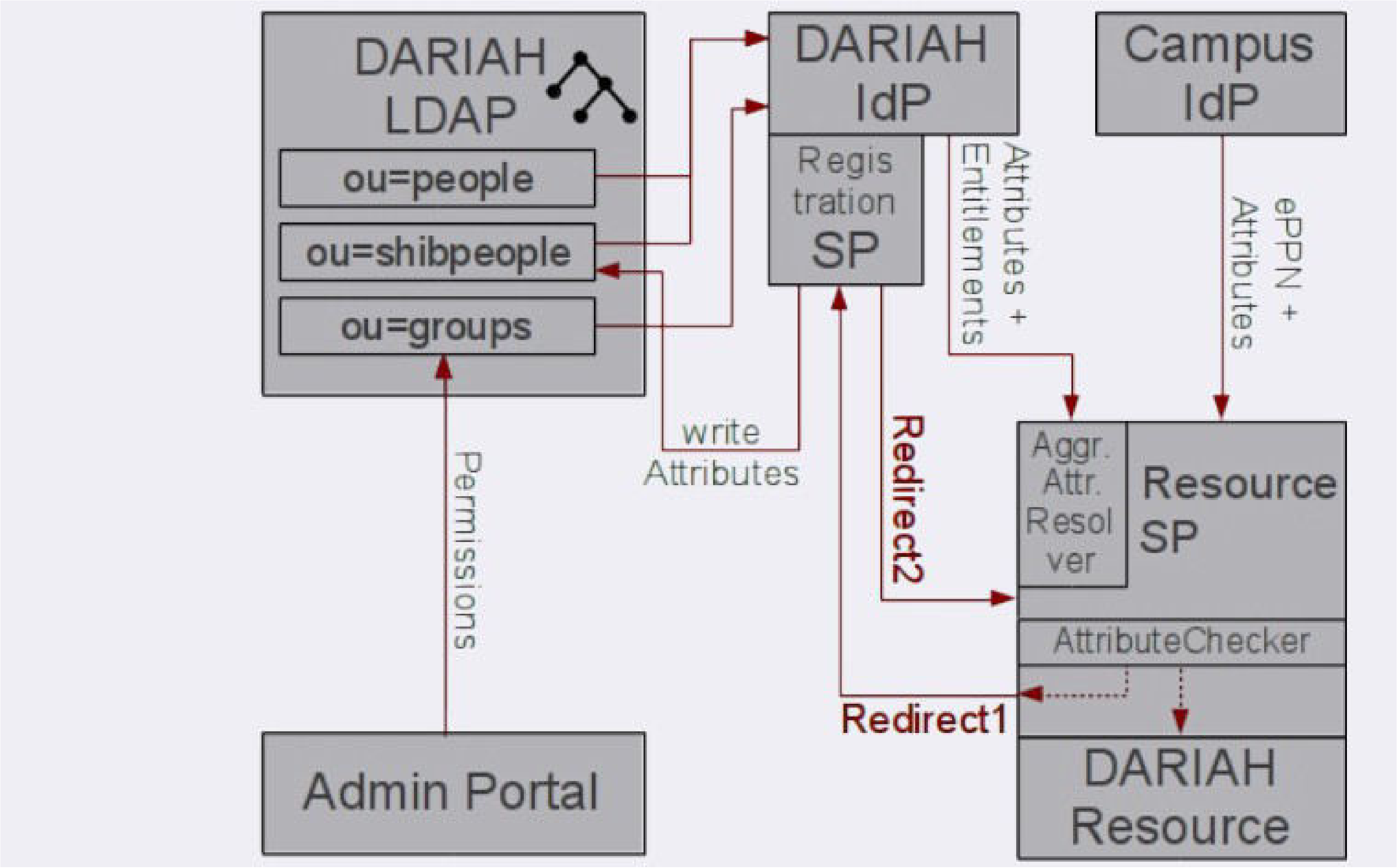
DARIAH AAI


GWDG
RZ Garching
OpenLDAP
http://www.OpenLDAP.org
LDAP
Replication
OpenLDAP
http://www.OpenLDAP.org
LDAP
Admin Portal
Self-service pwreset
Service Provider
Federation
DARIAH Identity Provider
Campus Identity Provider
Shibboleth
A Project of the Internet2 Middleware Initiative
LDAP
SAML

DARIAH AAI - challenges

- Goal 1: users of DARIAH services (SPs) should authenticate via their home organization (campus IdP).
- Goal 2: certain DARIAH services only allow particular user groups. This should be configurable centrally by the respective admins, for all DARIAH services.
- Goal 3: DARIAH needs some user information
  - 3.a) she agrees to DARIAH Terms
  - 3.b) she is a researcher (e.g. her organization or e-mail)
- Goal 4: cope with a situation where users either
  - 4.a) have no campus IdP
  - 4.b) their campus IdP would not release Personally Identifiable Information (PII) to hitherto unknown SPs

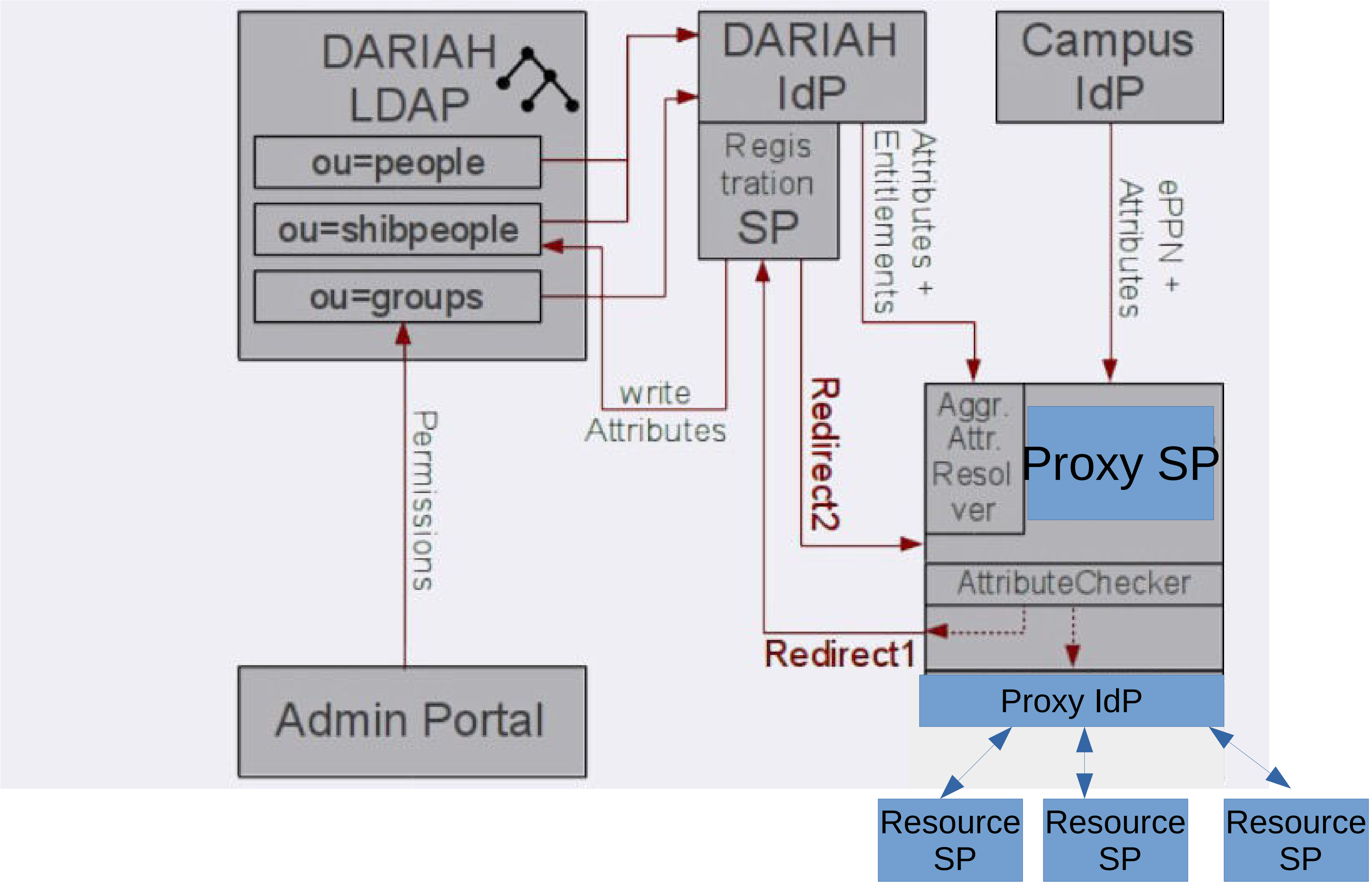
DARIAH AAI


DARIAH LDAP
ou=people
ou=shibpeople
ou=groups
DARIAH IdP
Campus IdP
Regis tration SP
Attributes + Entitlements
ePPN + Attributes
write Attributes
Redirect2
Permissions
Aggr. Attr. Resol ver
Resource SP
AttributeChecker
Redirect1
Admin Portal
DARIAH Resource

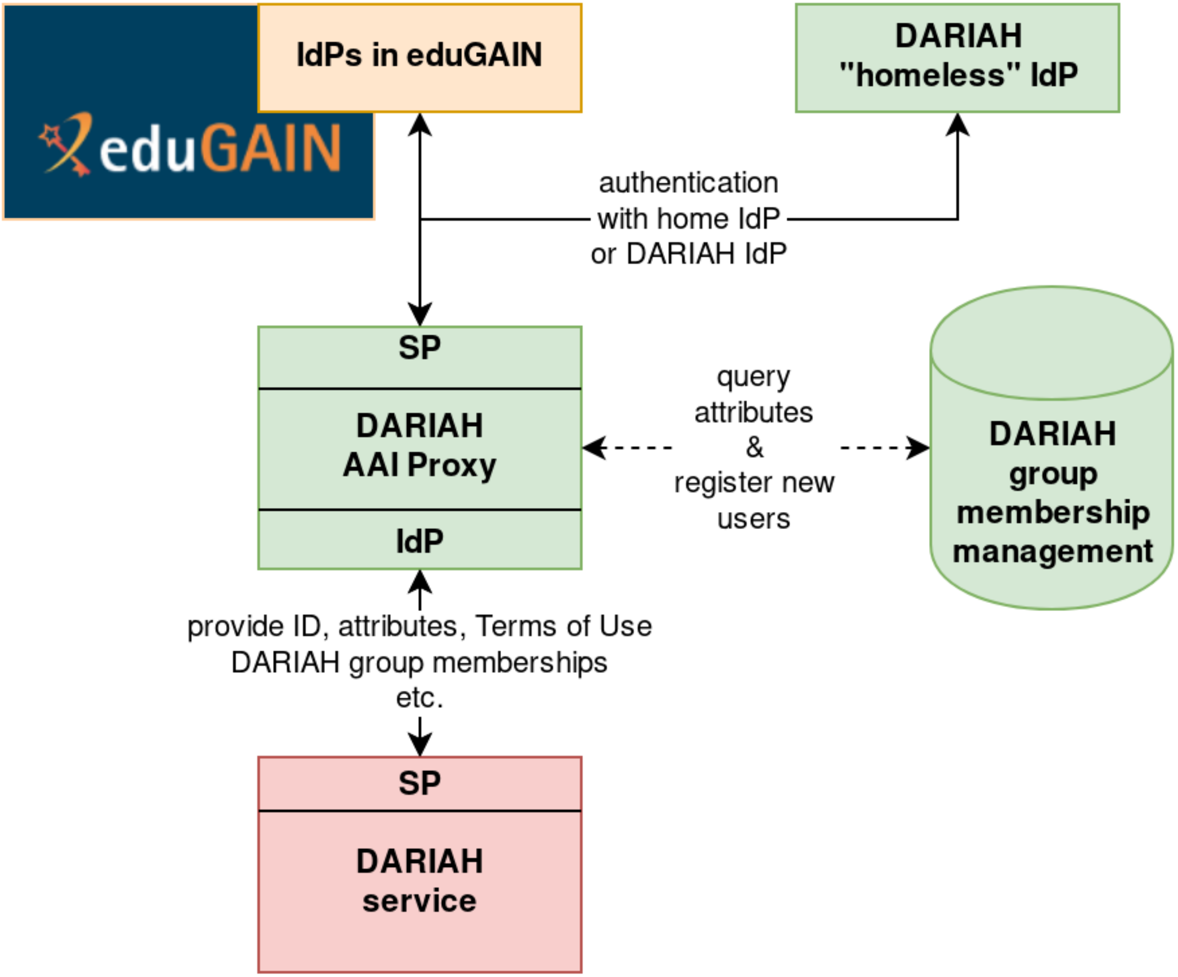
From AAI 1.0 to AAI 2.0

- In the past, it was difficult to connect services to the DARIAH Authentication and Authorization Infrastructure (AAI). In mid 2018, DARIAH introduced a central AAI proxy that brokers between DARIAH services and eduGAIN. The proxy took over many tasks from the services, which makes it much easier to connect new services to the DARIAH AAI.

DARIAH AAI NG



DARIAH AAI 2.0



IdPs in eduGAIN

DARIAH "homeless" IdP

authentication with home IdP or DARIAH IdP

SP

DARIAH AAI Proxy

IdP

query attributes & register new users

DARIAH group membership management

provide ID, attributes, Terms of Use DARIAH group memberships etc.

SP

DARIAH service

DARIAH AAI 2.0

- The proxy model is compliant with the AARC JRA1 Blueprint Architecture
- Runs in production since July 2018
- Already before the Proxy a lot of DARIAH services had implemented the more complicated non-proxied SP
- Now that we made connecting much easier, we expect even faster uptake
- Now it is also easier to support things like sirtfi and to integrate with other infrastructures, as EGI
- EGI interoperation PoC is running already

Connecting Services

- Almost any SAML Service Provider (SP) library can be used for an application
- No registration of the SP in a federation needed anymore - just exchange SAML metadata with the proxy
- The proxy ensures Identity Provider (IdP) Discovery and the connection to eduGAIN
- It provides services with all IdP attributes, plus information from the central DARIAH directory

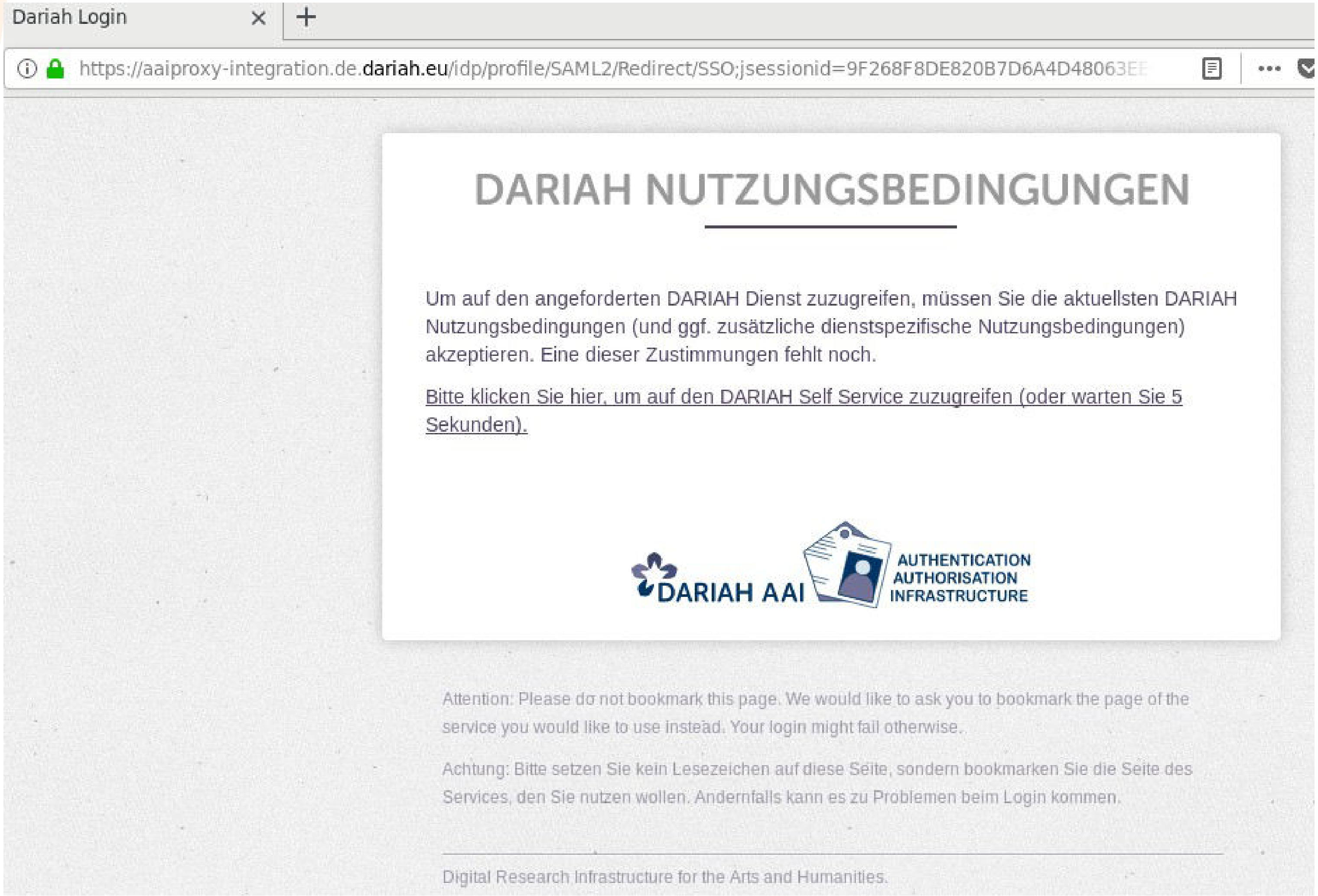
Inside the DARIAH AAI Proxy

- The DARIAH AAI proxy is based on the open source *Shibboleth* IdP and SP software. It implements the Blueprint Architecture of the Horizon 2020 AARC project and consists of:
  - IdP component that is connected to all DARIAH Services
  - SP component that is connected to all IdPs in eduGAIN.
- These two components are strung together, such that the AAI proxy forwards all data from eduGAIN IdPs on to DARIAH SPs.

Not just a Proxy

- Besides just forwarding IdP attributes, the DARIAH AAI proxy does a bit more to ensure DARIAH needs:
- Check if the eduGAIN user is registered in the DARIAH directory, and send her to the DARIAH Self-Service
- Check the DARIAH and possibly service-specific Terms of Use have been accepted
- Enrich IdP attributes with central authorization group information to be used for access control in services

Terms of Use Check



https://aaiproxy-integration.de.dariah.eu/idp/profile/SAML2/Redirect/SSO;jsessionid=9F268F8DE820B7D6A4D48063EE

DARIAH NUTZUNGSBEDINGUNGEN

Um auf den angeforderten DARIAH Dienst zuzugreifen, müssen Sie die aktuellsten DARIAH Nutzungsbedingungen (und ggf. zusätzliche dienstspezifische Nutzungsbedingungen) akzeptieren. Eine dieser Zustimmungen fehlt noch.

Bitte klicken Sie hier, um auf den DARIAH Self Service zuzugreifen (oder warten Sie 5 Sekunden).

DARIAH AAI
AUTHENTICATION
AUTHORISATION
INFRASTRUCTURE

Attention: Please do not bookmark this page. We would like to ask you to bookmark the page of the service you would like to use instead. Your login might fail otherwise.

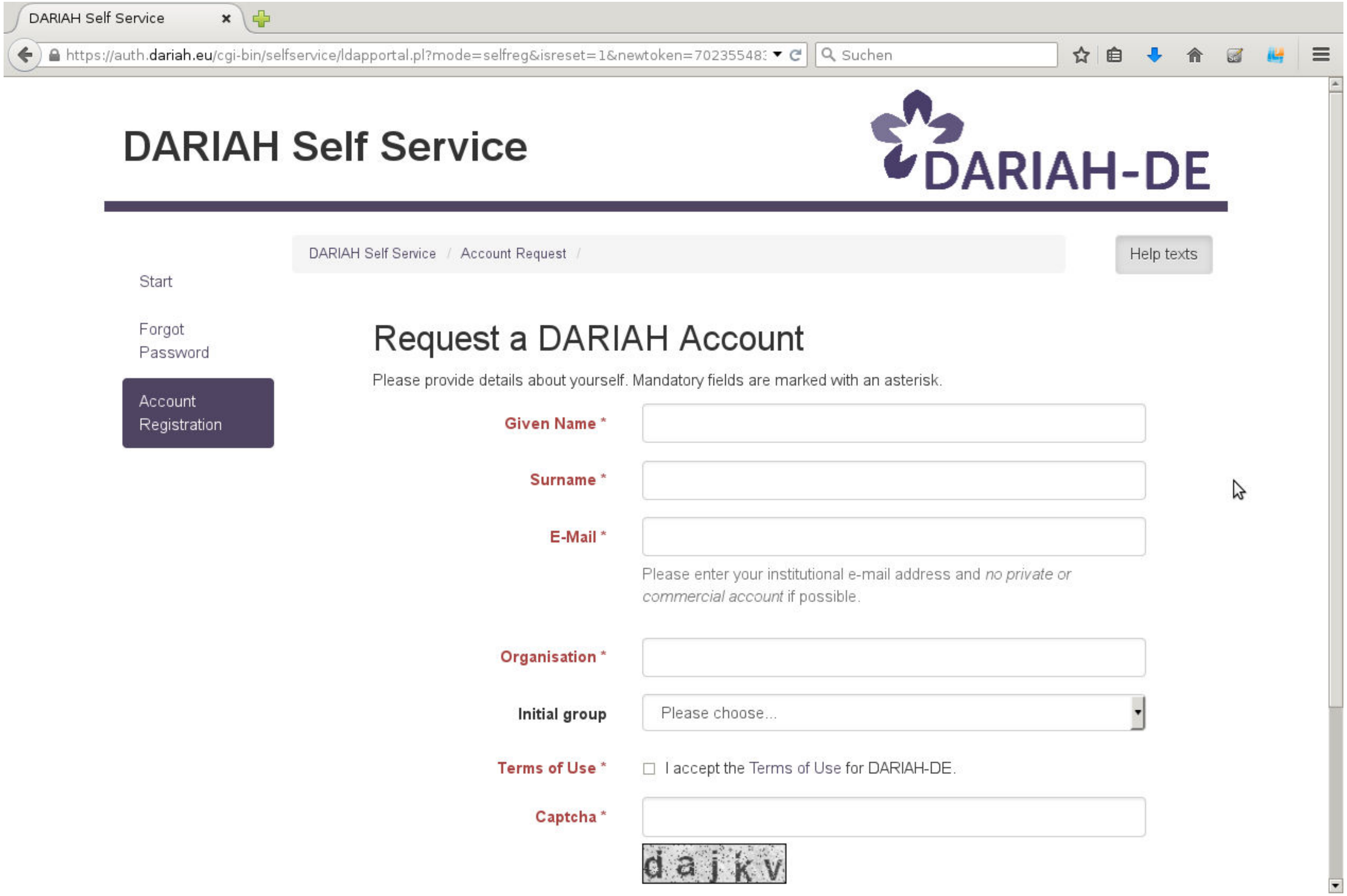
Achtung: Bitte setzen Sie kein Lesezeichen auf diese Seite, sondern bookmarken Sie die Seite des Services, den Sie nutzen wollen. Andernfalls kann es zu Problemen beim Login kommen.

Digital Research Infrastructure for the Arts and Humanities.

DARIAH SelfService

- Visit the DARIAH Self-Service at auth.de.dariah.eu that complements the proxy:
- Register users that authenticate via the eduGAIN meta-federation
- Let users agree to the general DARIAH and specific service Terms of Use
- Manage user's data in DARIAH
- Manage central authorization groups which services can use for access control
- For users that don not have an eduGAIN IdP: apply for DARIAH accounts and manage passwords

DARIAH AAI - Self Service



DARIAH Self Service
https://auth.dariah.eu/cgi-bin/selfservice/ldapportal.pl?mode=selfreg&isreset=1&newtoken=70235548:
Suchen
DARIAH-DE

DARIAH Self Service

DARIAH Self Service / Account Request /

Help texts

Start

Forgot Password

Account Registration

Request a DARIAH Account

Please provide details about yourself. Mandatory fields are marked with an asterisk.

Given Name *

Surname *

E-Mail *

Please enter your institutional e-mail address and *no private or commercial account* if possible.

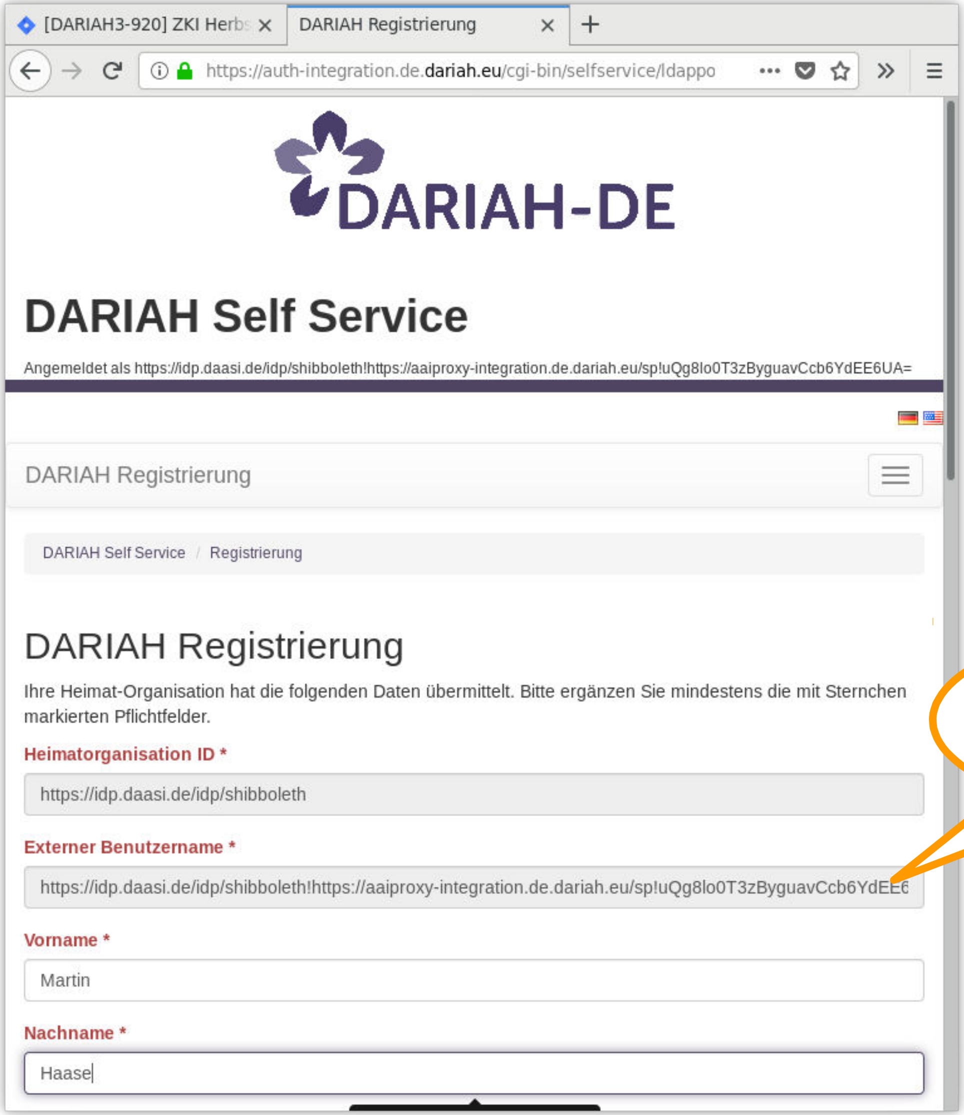
Organisation *

Initial group: Please choose...

Terms of Use * □ I accept the Terms of Use for DARIAH-DE.

Captcha *

DARIAH AAI - Register Federation Users


[DARIAH3-920] ZKI Herbs
DARIAH Registrierung
https://auth-integration.de.dariah.eu/cgi-bin/selfservice/ldappo
DARIAH-DE

DARIAH Self Service

Angemeldet als https://idp.daasi.de/idp/shibboleth!https://aaiproxy-integration.de.dariah.eu/sp!uQg8lo0T3zByguavCcb6YdEE6UA=

DARIAH Registrierung
DARIAH Self Service / Registrierung

DARIAH Registrierung

Ihre Heimat-Organisation hat die folgenden Daten übermittelt. Bitte ergänzen Sie mindestens die mit Sternchen markierten Pflichtfelder.

Heimatorganisation ID *
https://idp.daasi.de/idp/shibboleth

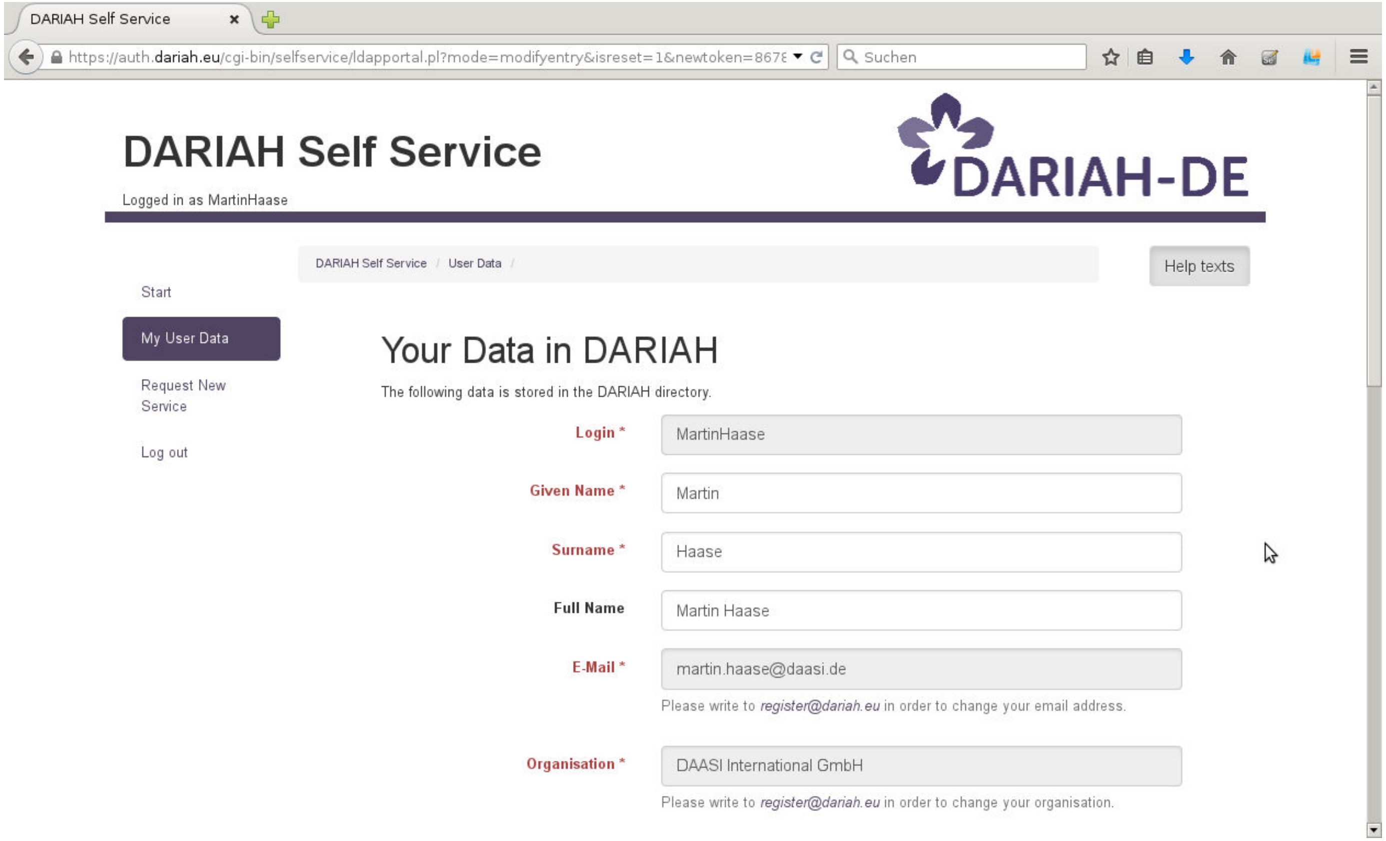
Externer Benutzername *
https://idp.daasi.de/idp/shibboleth!https://aaiproxy-integration.de.dariah.eu/sp!uQg8lo0T3zByguavCcb6YdEE6

Vorname *
Martin

Nachname *
Haase

Targeted / Persistent ID

DARIAH AAI - Self Service



DARIAH Self Service
https://auth.dariah.eu/cgi-bin/selfservice/ldapportal.pl?mode=modifyentry&isreset=1&newtoken=8678
Suchen

DARIAH Self Service

Logged in as MartinHaase

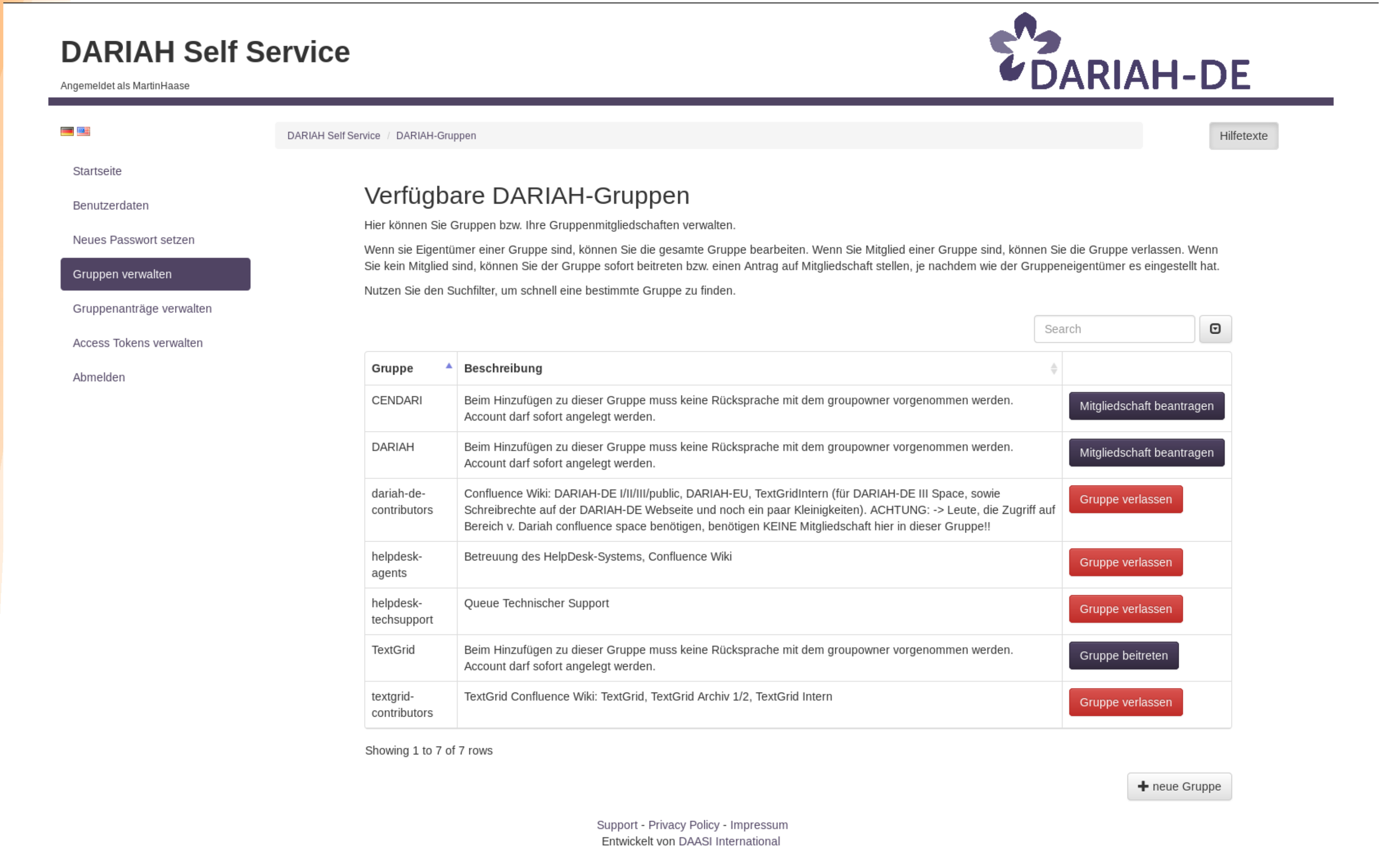
DARIAH-DE
DARIAH Self Service / User Data /
Help texts
Start
My User Data
Request New Service
Log out

Your Data in DARIAH

The following data is stored in the DARIAH directory.

Login *	MartinHaase
Given Name *	Martin
Surname *	Haase
Full Name	Martin Haase
E-Mail *	martin.haase@daasi.de Please write to *register@dariah.eu* in order to change your email address.
Organisation *	DAASI International GmbH Please write to *register@dariah.eu* in order to change your organisation.

DARIAH AAI - Administration: AuthZ Groups



DARIAH Self Service

Angemeldet als MartinHaase

DARIAH Self Service / DARIAH-Gruppen

Verfügbare DARIAH-Gruppen

Hier können Sie Gruppen bzw. Ihre Gruppenmitgliedschaften verwalten.

Wenn sie Eigentümer einer Gruppe sind, können Sie die gesamte Gruppe bearbeiten. Wenn Sie Mitglied einer Gruppe sind, können Sie die Gruppe verlassen. Wenn Sie kein Mitglied sind, können Sie der Gruppe sofort beitreten bzw. einen Antrag auf Mitgliedschaft stellen, je nachdem wie der Gruppeneigentümer es eingestellt hat.

Nutzen Sie den Suchfilter, um schnell eine bestimmte Gruppe zu finden.

Gruppe	Beschreibung	
CENDARI	Beim Hinzufügen zu dieser Gruppe muss keine Rücksprache mit dem groupowner vorgenommen werden. Account darf sofort angelegt werden.	Mitgliedschaft beantragen
DARIAH	Beim Hinzufügen zu dieser Gruppe muss keine Rücksprache mit dem groupowner vorgenommen werden. Account darf sofort angelegt werden.	Mitgliedschaft beantragen
dariah-de-contributors	Confluence Wiki: DARIAH-DE I/II/III/public, DARIAH-EU, TextGridIntern (für DARIAH-DE III Space, sowie Schreibrechte auf der DARIAH-DE Webseite und noch ein paar Kleinigkeiten). ACHTUNG: -> Leute, die Zugriff auf Bereich v. Dariah confluence space benötigen, benötigen KEINE Mitgliedschaft hier in dieser Gruppe!!	Gruppe verlassen
helpdesk-agents	Betreuung des HelpDesk-Systems, Confluence Wiki	Gruppe verlassen
helpdesk-techsupport	Queue Technischer Support	Gruppe verlassen
TextGrid	Beim Hinzufügen zu dieser Gruppe muss keine Rücksprache mit dem groupowner vorgenommen werden. Account darf sofort angelegt werden.	Gruppe beitreten
textgrid-contributors	TextGrid Confluence Wiki: TextGrid, TextGrid Archiv 1/2, TextGrid Intern	Gruppe verlassen

Showing 1 to 7 of 7 rows

Support - Privacy Policy - Impressum
Entwickelt von DAASI International

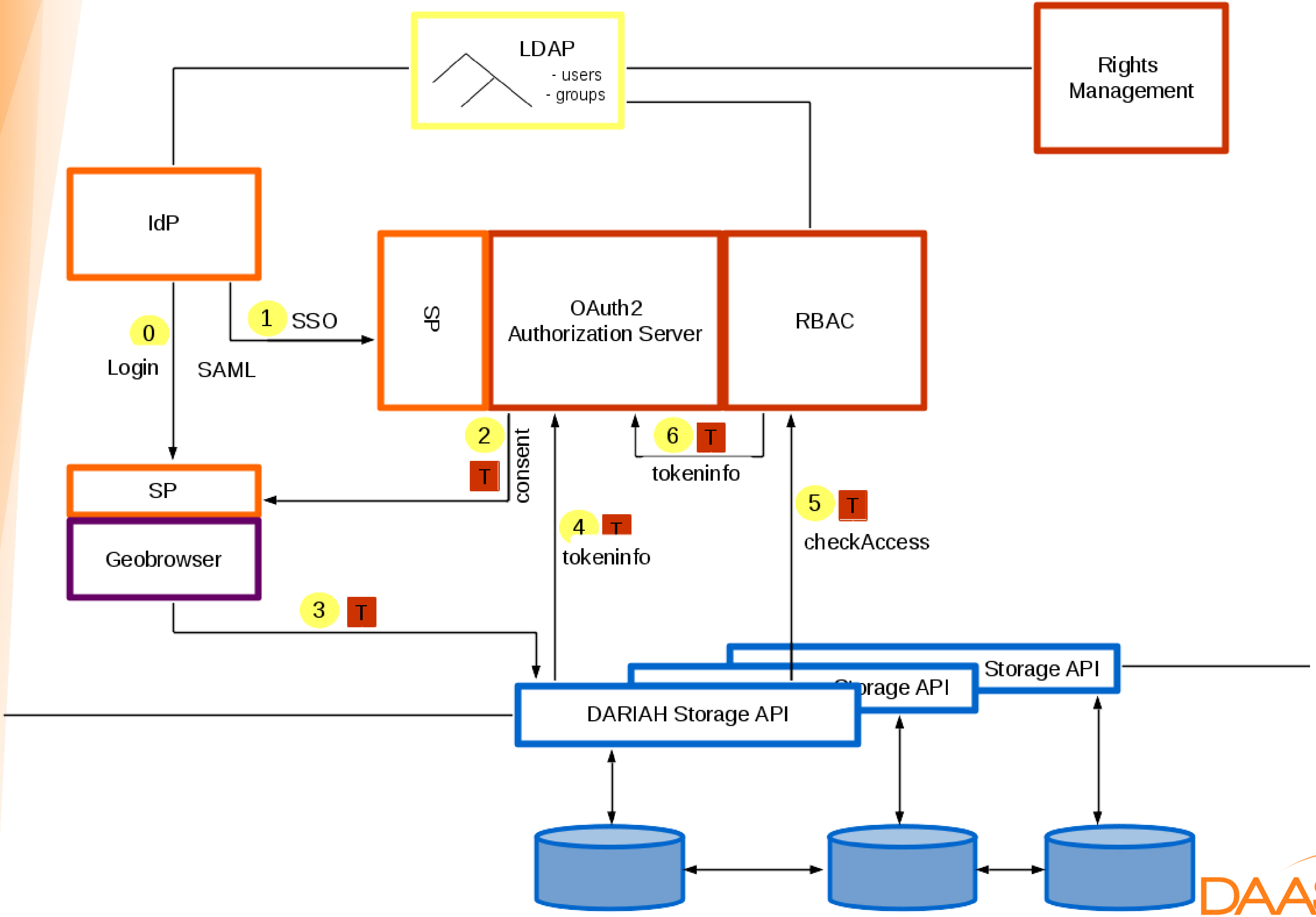
Zahlen (2018-08)

- > 4630 DARIAH-Nutzer
- > 390 DARIAH-Nutzer von 72 IdPs aus eduGAIN (plus CLARIN)
- 322 Benutzergruppen
- Every project usually uses three or four priviledge groups, thus ca. 85 projects (5 more)
  - X-users, X-contributors, [X-developpers], X-admins

Central Policy Decision Point

- If more than one system trusts an access policy it makes sence to have a central policy decision point
  - Manage the access rules only once
  - Policy Enforcement Point
    - doesn‘t have to deal with managing and evaluating access policy
    - Just needs to get access decisions from the PDP via simple and standardized protocols
- DARIAH uses the RBAC compliant open-source PDP „didmos Decision Point“ in combination with apis OAuth2 Authorization Server

DARIAH PDP


LDAP
- users
- groups
Rights
Management
IdP
1
SSO
0
Login
SAML
SP
OAuth2
Authorization Server
RBAC
2
T
consent
6
T
tokeninfo
SP
Geobrowser
4
T
tokeninfo
5
T
checkAccess
3
T
Storage API
Storage API
DARIAH Storage API

PDP - Flow

- 0: Session mit einem OAuth2-fähigen Dienst besteht
- 1: Redirect mit SAML-Login am OAuth2 AS
- 2: AS erfragt Consent, und schickt Redirect mit Token (evtl AuthZ Code noch davor) zurück zum Dienst
- 3. Dienst setzt Token ein, Resource: StorageAPI
- 4. StorageAPI holt sich UserID aus Token
- 5. StorageAPI fragt PDP: checkAccess(UserID,read/write/operationABC,DateiXYZ)
- 6. Interne Token-Validierung (PDP beim AS)
- Auslieferung der DateiXYZ an Dienst

Connect the SP to the DARIAH AAI

DAASI International

Set up Trust with the AAI Proxy

- Download the DARIAH AAI Proxy's Metadata file like this (mind the capital "-O")

```
wget https://aaiproxy.de.dariah.eu/idp
-O /etc/shibboleth/dariah-proxy-idp.xml
```

- Locate the MetadataProvider section in /etc/shibboleth/shibboleth2.xml and add a row:

```
<MetadataProvider type="XML" file="dariah-
proxy-idp.xml"/>
```

- Send your own SP's metadata to register@dariah.eu (from https://your.sp.edu/Shibboleth.sso/Metadata)

Further SP Configuration

- In /etc/shibboleth/shibboleth2.xml, set the SP to direct login using

```
<SSO entityID="https://aaiproxy.de.dariah.eu/idp">
```

- Use the following ID preference order

```
REMOTE_USER="eppn unique-id"
```

- Enable eduPersonUniqueID in /etc/shibboleth/attribute-map.xml:

```
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.13"
            id="unique-id">

     <AttributeDecoder
            xsi:type="ScopedAttributeDecoder"/>

</Attribute>
```

Attributes in the DARIAH AAI

- Released by default: eppn, affiliation, unscoped-affiliation, entitlement
- Add and use unique-id for personalization (see previous slide)
- Configure in /etc/shibboleth/attribute-map.xml, by uncommenting: cn (CommonName), givenName, sn (surname), displayName, preferredLanguage, o (Organization), mail, schacCountryOfCitizenship
- DARIAH-specific Attributes, by adding:

```
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
id="isMemberOf"/>

<Attribute name="urn:oid:1.3.6.1.4.1.10126.1.52.5.2"
id="dariahRole"/>

<Attribute name="urn:oid:1.3.6.1.4.1.10126.1.52.4.15"
id="dariahTermsOfUse"/>
```

Attributes from Campus IdPs

- Adapt attribute-policy.xml to accept any scope
- Remove the Scope Checking stanza for affiliation and eppn

```
<afp:AttributeRule attributeID="affiliation">
            <afp:PermitValueRule xsi:type="AND">
                <RuleReference ref="eduPersonAffiliationValues"/>
<!-- accept any scope  <RuleReference ref="ScopingRules"/> -->
            </afp:PermitValueRule>
 </afp:AttributeRule> [...]
<!-- accept any scope for legacy users
        <afp:AttributeRule attributeID="eppn">
            <afp:PermitValueRuleReference ref="ScopingRules"/>
        </afp:AttributeRule> -->
```

Terms of Use for Service

- Generally DARIAH AAI ToU must be accepted by anyone using the DARIAH AAI
- The AAI proxy checks the ToU acceptance
- A DARIAH Service can have *additional* ToU
- Upload your ToU document to the DARIAH Repository, cf. DARIAH ToU:

https://repository.de.dariah.eu/1.0/dhcrud/21.11113/0000-000B-CB44-4

Terms of Use for Service (2)

- Then request an *authorization group* attached with your service's ToU:
- Log in to the SelfService, and choose
  - Manage Groups
  - "+ new group" (at the bottom of the page)
  - Choose a group name, e.g. ***myservice-users***
  - Put the link to your ToU in the "Remarks" box
- DARIAH staff will create the group for you

Thanks!

https://www.daasi.de