What is DARIAH?

DARIAH: Digital Research Infrastructure for the Arts and Humanities

One of the few ESFRI research infrastructures for the humanities (**ERIC is in working mode by now**)

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
Current AAI set-up: a first version of an AA infrastructure has been deployed, based on two standards:

- **LDAP (Lightweight Directory Access Protocol)**
  - for authentication and authorization attributes
  - deploying Open Source Software OpenLDAP
- **SAML (Security Assertions Markup Language)**
  - for AAI within a federation
  - including Web Single Sign-On feature
  - deploying Open Source Software Shibboleth
DARIAH AAI Setup

**Diagram Description:**
- **GWDG**
  - LDAP
  - Admin Portal
  - Self-service pwreset

- **JIRA**
- **Confluence**

- **RZ Garching**
  - LDAP
  - Federation
  - DARIAH Identity Provider
  - Campus Identity Provider
  - Service Provider

- **Replication**

- **OpenLDAP**

- **LDAP**
- **SAML**
VO Management and FIM in DARIAH
VO Management and FIM in DARIAH

SP Proxy will make it easier for DARIAH Services to join
Current Challenge

- European-wide federation eduGain has too little outreach
- Not every institution signs federation contracts
- Not every Identity Provider releases personal attributes
- Technologies for non-web-based access only “almost there” (ECP, STS, Moonshot, oAuth2)
- Fine grained access control on file level, observed within a data replication federation (= non web SSO)
New Access Control Architecture

OAuth2 Client Credentials Grant
Self-contained Access+Refresh Tokens
Server-hosted Application

DARIAH IdP

1. User Attrs

2. AuthZ Attrs

Browser

DARIAH Rep

3. Client Credentials + UserID

4. Access

5. ValidateToken

6. CheckAccess

DARIAH Storage API

1. Access

2. Access

DARIAH Storage API

IRODs Replication
Current figures

• We currently have >3100 Users (700 new since February)
• Still most do not log in via their home IdP
  • It's easier (and sort of familiar) to create a new DARIAH account
• We currently have >250 different user groups (40 new since February)
  • Every project usually uses three or four privileged groups (thus ca. 75 projects ca. 15 new since February):
    • X-users, X-contributors, [X-developpers], X-admins
How to make this a European-wide Infrastructure

• The management of the delegation is based on organisational roles (not groups) that are structured in a 3 level hierarchy:
  • DARIAH Coordination Office as Top of hierarchy
    • Each Country has a National Representative who is allowed to:
      • Create and manage organisations and the organisation admin role
    • Each Organisation in a country has a organisation admin
      • Organisation admin is allowed to:
        • Create and manage groups (of projects the organisation is leading)
        • Create 'homeless'-accounts if needed

Production ready Administration interface is there
New Features of User Management

- The Web-based administration and self-service interfaces have been improved, e.g.
  - Distributed user management
  - Better password forgotten processes
  - Completed role based administration
  - Concept of initial group is implemented
- Since the administration interface is actually used, new requirements pop up quite often
Screenshots of Selfservice and Administration interface
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** *
  
  [Image: Image of a CAPTCHA]

- **Remarks**

Visit the DARIAH Wiki
© DAASI International
Login to the System

Please enter Login Name and Password

Login
Password

Visit the DARIAH Wiki
© DAASI International
Select your session role

You have privileges on more than one subtree. Please select the subtree, you want to work on now.

subtree: National Representative, DE: organisations, dariah

Visit the DARIAH Wiki
© DAASI International
Complex Search

Please enter the search terms

Given Name
Surname
Login

Please select
- All fields must match
- Only one field must match

Start search
Group Management

You can edit the following groups:

<table>
<thead>
<tr>
<th>Group name</th>
<th>Owner</th>
<th>Modify</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>admins</td>
<td>uid=pgietz,ou=people,dc=darjah,dc=eu</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ag-netzpolitik-contributors</td>
<td>uid=groupowner,ou=dsa,dc=darjah,dc=de</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aib-admins</td>
<td>uid=groupowner,ou=dsa,dc=darjah,dc=de</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aib-contributors</td>
<td>uid=groupowner,ou=dsa,dc=darjah,dc=de</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aib-developers</td>
<td>uid=groupowner,ou=dsa,dc=darjah,dc=de</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aib-users</td>
<td>uid=groupowner,ou=dsa,dc=darjah,dc=de</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cendari-admins</td>
<td>uid=groupowner,ou=dsa,dc=darjah,dc=de</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cendari-contributors</td>
<td>cn=cendari-admins,ou=groups,dc=darjah,dc=eu</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cendari-user</td>
<td>cn=cendari-admins,ou=groups,dc=darjah,dc=eu</td>
<td></td>
<td></td>
</tr>
<tr>
<td>collection-registry-admins</td>
<td>uid=groupowner,ou=dsa,dc=darjah,dc=eu</td>
<td></td>
<td></td>
</tr>
<tr>
<td>collection-registry-contributors</td>
<td>uid=groupowner,ou=dsa,dc=darjah,dc=eu</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Account Requests

The following account requests exist in the system:

<table>
<thead>
<tr>
<th>Vorname</th>
<th>Name</th>
<th>Organisation</th>
<th>E-Mail</th>
<th>Begründung</th>
<th>Nr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find</td>
<td>Mich</td>
<td>asdfasdfsdf</td>
<td><a href="mailto:fm@daasi.de">fm@daasi.de</a></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>mir</td>
<td>egal</td>
<td>asdfasdf</td>
<td><a href="mailto:egal@daasi.de">egal@daasi.de</a></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>Verstecke</td>
<td>Mich</td>
<td>awefjant</td>
<td><a href="mailto:vm@daasi.de">vm@daasi.de</a></td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Willi</td>
<td>Nichi</td>
<td>werden</td>
<td><a href="mailto:gefunden@daasi.de">gefunden@daasi.de</a></td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Und</td>
<td>ich</td>
<td>will</td>
<td><a href="mailto:ul@daasi.de">ul@daasi.de</a></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Minimaler</td>
<td>Account</td>
<td>Da wir keine Organisation haben, erstmal Freitext.</td>
<td><a href="mailto:minimak@daasi.de">minimak@daasi.de</a></td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>Maximaler</td>
<td>Account</td>
<td>Nach eine Organisation</td>
<td><a href="mailto:maximal@daasi.de">maximal@daasi.de</a></td>
<td></td>
<td>13</td>
</tr>
<tr>
<td>Neu</td>
<td>Maximal</td>
<td>Fasdfsfd</td>
<td><a href="mailto:neumax@daasi.de">neumax@daasi.de</a></td>
<td></td>
<td>14</td>
</tr>
<tr>
<td>Hadschi</td>
<td>Al-Arab</td>
<td>asdfdfjasdf</td>
<td><a href="mailto:hasch@daasi.de">hasch@daasi.de</a></td>
<td></td>
<td>15</td>
</tr>
<tr>
<td>asdfjdasdf</td>
<td>asdfasdf</td>
<td>asdfdsd</td>
<td><a href="mailto:asdfgasdfg@daasi.de">asdfgasdfg@daasi.de</a></td>
<td></td>
<td>16</td>
</tr>
<tr>
<td>Mursks</td>
<td>Maskr</td>
<td>alsdqaikjd</td>
<td><a href="mailto:asdhj@daasi.de">asdhj@daasi.de</a></td>
<td></td>
<td>17</td>
</tr>
<tr>
<td>Sowieso</td>
<td>was</td>
<td>asdfijk</td>
<td><a href="mailto:asdfgasdfg@daasi.de">asdfgasdfg@daasi.de</a></td>
<td></td>
<td>18</td>
</tr>
</tbody>
</table>
DARIAH Account Administration

Logged in as Martin Haase, National Representative - DE

Account Requests

![Responsive design](https://dariah-daasi.de/cgi-bin/admin/ldapportal.pl?m)

Organisations / Account Requests /

Account Requests

The following account requests exist in the system.

<table>
<thead>
<tr>
<th>Vorname</th>
<th>Name</th>
<th>Organisation</th>
<th>E-Mail</th>
<th>Begründung</th>
<th>Nr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find</td>
<td>Mich</td>
<td>asdfasdfs</td>
<td><a href="mailto:fmf@daasi.de">fmf@daasi.de</a></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>mir</td>
<td>egal</td>
<td>asdfgasdfs</td>
<td><a href="mailto:egal@daasi.de">egal@daasi.de</a></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>Verstecke</td>
<td>Nichi</td>
<td>awetjanf</td>
<td>vr@<a href="mailto:g@daasi.de">g@daasi.de</a></td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Willi</td>
<td>Niki</td>
<td>werden</td>
<td><a href="mailto:gefunden@daasi.de">gefunden@daasi.de</a></td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Und</td>
<td>ich</td>
<td>will</td>
<td><a href="mailto:uli@daasi.de">uli@daasi.de</a></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Minimaler</td>
<td>Account</td>
<td>Dabei meine Organisation haben, erstmal Freitext.</td>
<td><a href="mailto:minimal@daasi.de">minimal@daasi.de</a></td>
<td></td>
<td>12</td>
</tr>
</tbody>
</table>
DARIAH Account Administration

Logged in as Martin-loese, DCD-admin - organisations

Home Page
Search
Complex Search
New Account
Groups
New Country
LDAP Statistics
Countries
Account Requests
Change Role
Log Out

Browse in tree
you can browse through your subtree

Current entry:

- DE, organisations, daria
- IT, organisations, daria
- NL, organisations, daria
- GB, organisations, daria
- IR, organisations, daria
- GR, organisations, daria
- BE, organisations, daria

Visit the DARIAH Wiki
© DAASI International
Modify country

Please modify the country data

- Land: UNITED KINGDOM
- Description: Great Britain
- National Representative: uid=MartinHaase.eu=people,dc=dariah,dc=eu

[cancel] [add national representative] [save]
New Group Member (Make selected to GB)

The following entries were found:

<table>
<thead>
<tr>
<th>Vorname</th>
<th>Name</th>
<th>Login</th>
<th>Affiliation</th>
<th>Abteilung</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>Martin</td>
<td>Haase</td>
<td>MartinHaase</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DAASI International</td>
<td></td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GmbH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td>Martin</td>
<td>Haase</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DAASI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td>Martin</td>
<td>Haase</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Thaleheim</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Select all ☐

Visit the DARIAH Wiki
© DAASI International
Create new account, step 1: check for existence

Please enter your search terms

Given Name: Henry
Surname: Hubble

Enter your surname or family name.
Check for existence
Create New Account

Please enter the user's data

- **Login**
  - Will be created automatically if this field is left empty.

- **Surname**
  - Hubble

- **Given Name**
  - Henry

- **E-Mail**

- **Organisation**

- **Language**
  - German
  - English

- **Activation data**
  - Notification of new account will be sent at that date. Will be sent immediately if empty.

- **Deletion data**
  - Account will be deleted at that date. Will not be deleted automatically if empty.

- **Initial group**
  - Please choose

- **Description**
Create New Organisation

Please enter the organisation's data

**Organisation**: King's College London

**Description**: Some description

**Orgadmin**

[save] [save and add organisation administrator]

Visit the DARIAH Wiki
© DAASI International
Modify Organisation

Please modify the organisation's data

Organisation: King's College London

Description: Some description

Orgadmin: uid=MartinHaase,ou=people,dc=dariah,dc=eu

[Buttons: cancel, add orgadmin, save]
Sustainability

• There is the strong will to make DARIAH a sustainable infrastructure

• One of the 6 Project Cluster of DARIAH-DE is DARIAH eHumanities Infrastructure Service Unit (DeISU)
  • We will be working on organizational model and business model
  • That service unit could well also operate AAI services
Service Providers (SPs)

Service Providing Contracts for DARIAH SPs
Including SLAs and ToU

DeISU and its services

Service Providing Contract for users
Including SLAs and ToU

User Institutions

Users
Summary

- DARIAH has a productive solution based on homeless-IdP and attribute authority
- Distributed user and priviledge administration
- Roadmap for a sustainable service unit
- Policies that allow for integration into DFN-AAI and thus into eduGain
- DARIAH is actively co-operating with AARC
Thank you for listening!

Questions?

Comments?