DARIAH-AAI

DASISH AAI Meeting

Nijmegen, March 9th, 2014

DARIAH-EU

DAASI International

www.dariah.eu

What is DARIAH?

DARIAH: Digital Research Infrastructure for the Arts and Humanities

One of the few ESFRI research infrastructures for the humanities

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

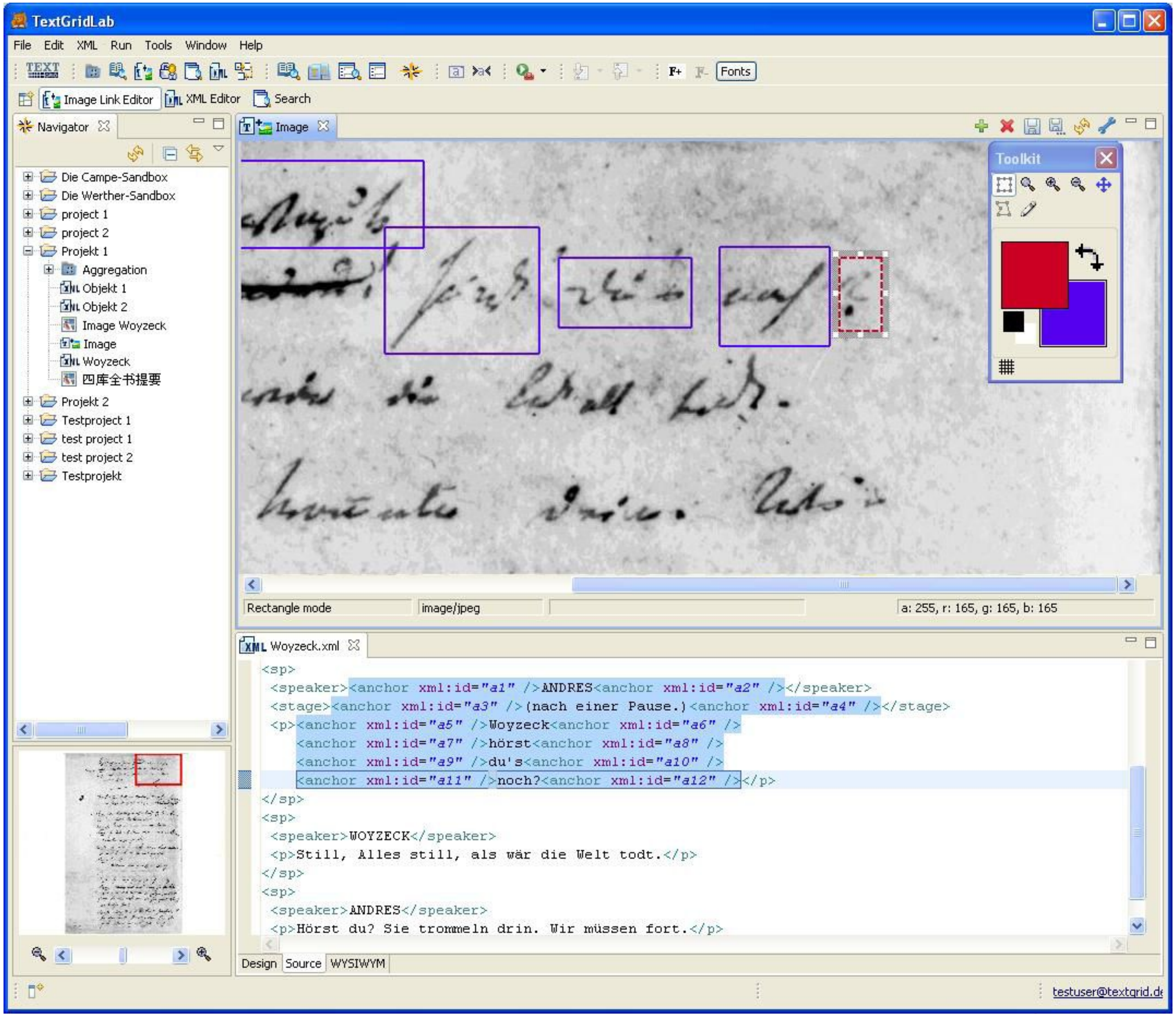
Working with communities of practice: humanities scholars supporting their VREs

DARIAH-EU

DAASI International

Humanities VRE

TextGrid



```
<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</speaker>
 <p>Still, Alles still, als wär die Welt todt.</p>
</sp>
<sp>
 <speaker>ANDRES</speaker>
 <p>Hörst du? Sie trommeln drin. Wir müssen fort.</p>
```

DARIAH-EU

DARIAH AAI Practice

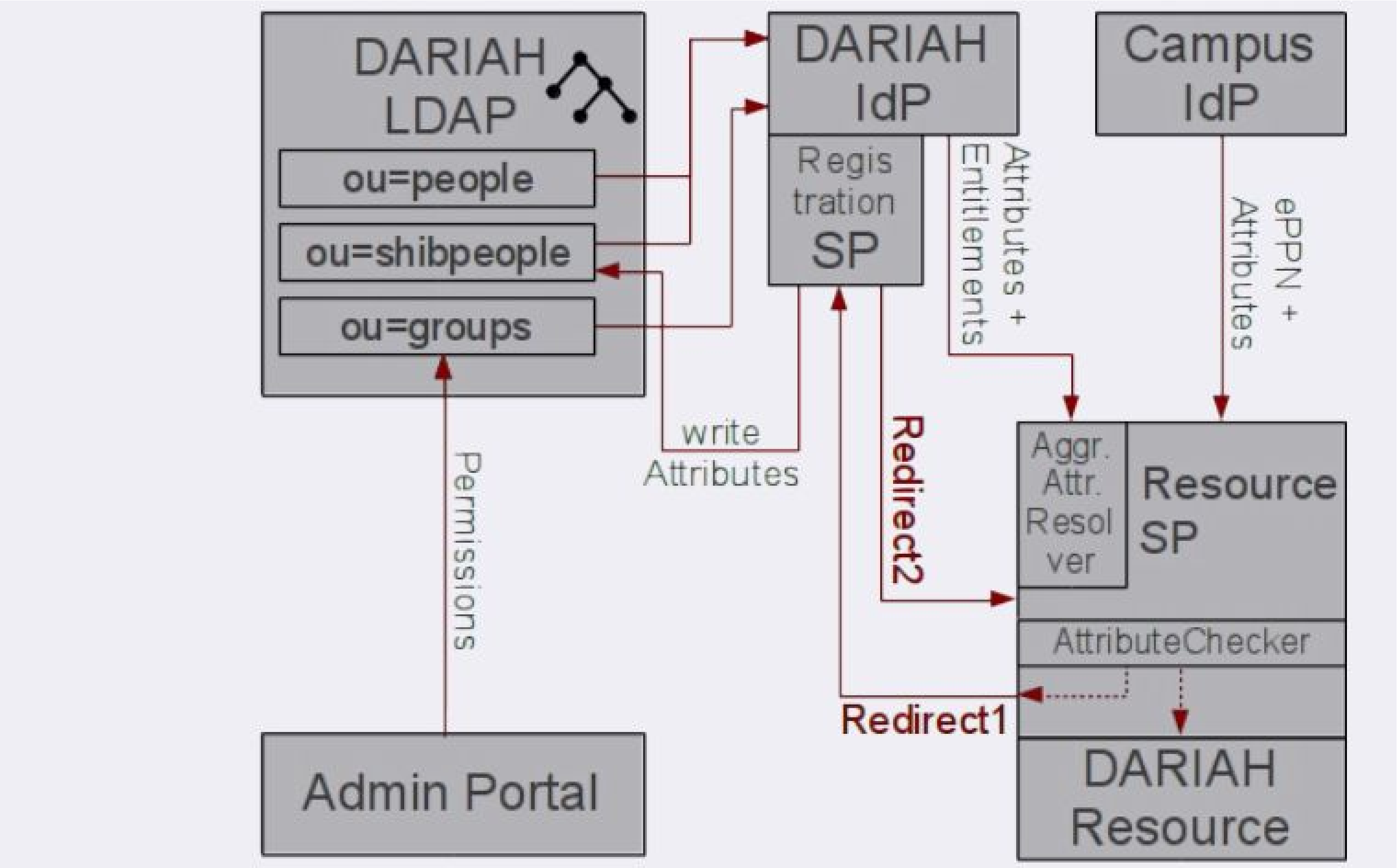
Current AAI set-up: a first version of an AA infrastructure has been deployed, based on two standards:

- LDAP (Lightweight Directory Acess 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 Autorization

- Use of the Higher-Education SAML-based federations
- No change to campus IdPs except trust / attribute filters
- Standard Shibboleth SP to protect DARIAH applications, however with special configuration:
  - aggregates attributes from campus and central IdP
  - require miminum set of attributes, otherwise redirect to registration application at central SP
- Central LDAP with authZ groups managed by admin portal
- Central IdP gets data from central LDAP and releases both user attributes and entitlements (based on groups) to SPs
- Central Registration SP writes manually completed user attributes to central LDAP

VO Management and FIM in DARIAH



DARIAH-EU

DAASI International

Current Challenge

– Not every institution signs federation contracts

– Not every Identity Provider releases personal attributes

– Not every resource provider allows anonymous usage

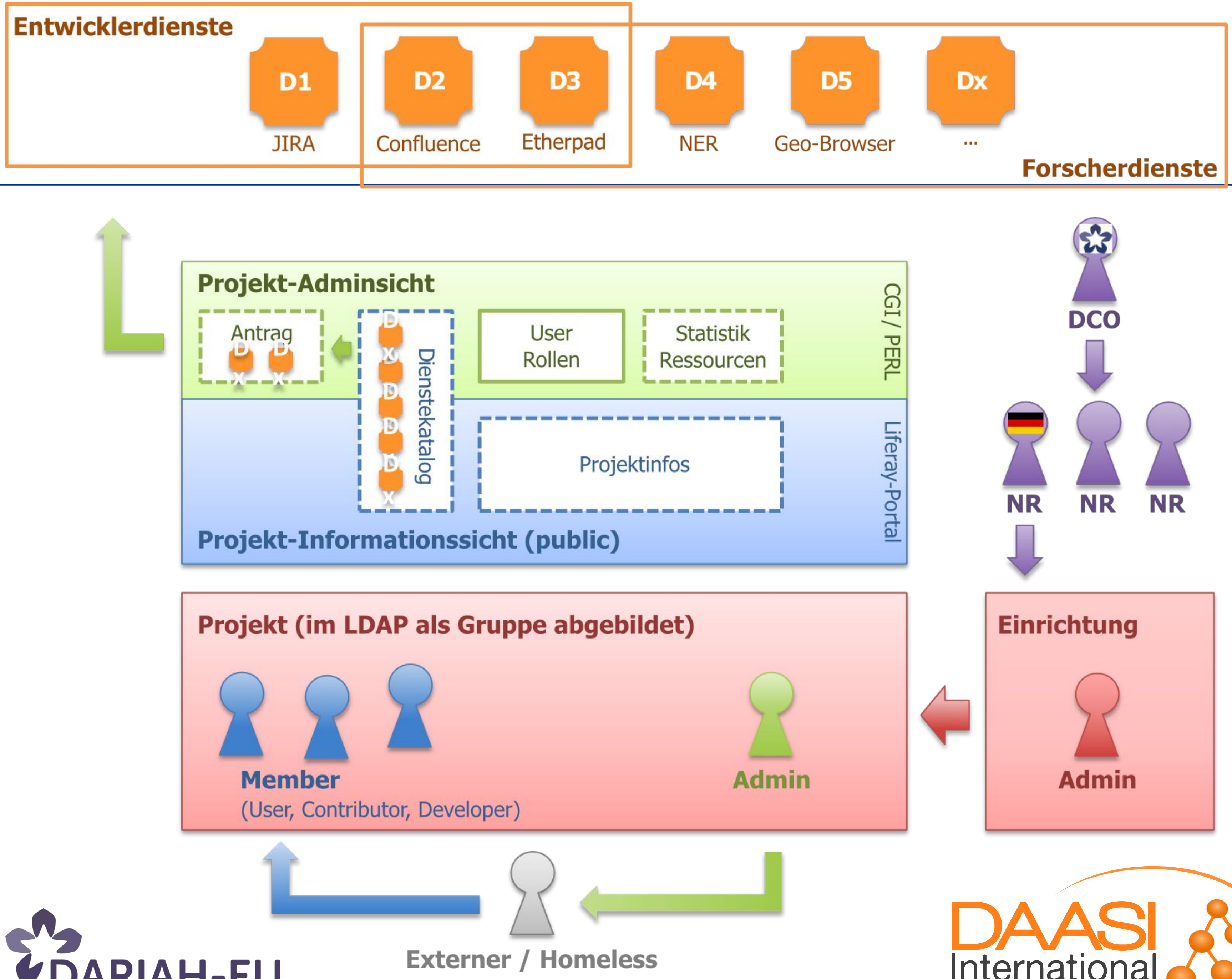
– A European humanities federation is just at its start (CLARIN federation, DASISH activities)

How to make this a European-wide Infrastructure?

- We have productive a 'flat' Group based Authorization:
  - You are member of group
    - EHRI-users allowes to access the EHRI part of the DARIAH wiki
    - collection-registry-users allowes to use the collection registry
    - collection-registry-editors allowes to input data into the registry
    - collection-registry-admins allowes to configure the registry
    - Collection-registry-groupadmins allowes to manage all groups with names beginning with 'collection registry-'
- So how to delegate the groupadmins-rights?
  - We developed and implemented a hierarchical role model to delegate user rights management

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 (marked ⬢):
- ⬢ 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



Entwicklerdienste

D1 JIRA

D2 Confluence

D3 Etherpad

D4 NER

D5 Geo-Browser

Dx …

Forscherdienste

Projekt-Adminsicht

Antrag

Dx Dx

Dienstekatalog

Dx Dx Dx Dx Dx

User Rollen

Statistik Ressourcen

CGI / PERL

Projektinfos

Liferay-Portal

Projekt-Informationssicht (public)

DCO

NR NR NR

Projekt (im LDAP als Gruppe abgebildet)

Member

(User, Contributor, Developer)

Admin

Einrichtung

Admin

Externer / Homeless

DARIAH-EU

DAASI International

How to make this a European-wide Infrastructure

- So software there, now we need to organize it:
  - Who will be National Representative
  - What shall she be able to do except creating organisations and orgadmin roleoccupantships?
  - What will the organizational application process look like?
  - What more data do we need about the users
    - By now: Name, email, preferred language, affiliation
    - Should we add ORCID-IDs?

How to get the urgently needed European humanities federation?

- By now the demonstrated infrastructure is only accessile via DFN-AAI or via a dedicated DARIAH and TextGrid ('homeless')-Account.
- EduGain, the European federation of national federations is evolving

How to get the urgently needed European humanities federation?

Two ways forward:

- A) DARIAH IdPs and SPs either participate via the national federations
- B) Or they create (together with CLARIN and other DASISH partners) a humanities federation that can become member of eduGain

A GÉANT 3 Plus Pilot project with DARIAH has started to evaluate these options

At the Humanities federation Workshop with DASISH partners October 17/18 in Cologne, we sort of decided to go for A for now and have B as Plan B

How to get into DFN-AAI

- DFN is very open for this
- Homeless IdP needs a documented policy
- SPs just need to sign the contracts
  - This is ongoing
  - Needs to be pushed and sometimes time is missing

Policy for Homeless IdP

- We already have > 500 user
- They came into the homeless IdP under an implicit policy
- Now we have an explicit policy and are in the process of purging the accounts
- This is being done while merging the TextGrid homeless IdP with the DARIAH IdP

Policy for Homeless IdP: Registration

- If the requester has an email adress from the scientific community (e.g. xxx@uni-yyy.de)
  - ok, no questions asked
- If email address is from a commercial provider:
  - Ask to use another email address
  - If this is not possible we have two problems:
    - A) Is the person the one she claims to be
    - B) Does the person belong to the scientofic community?

Policy for Homeless IdP: Registration

- A) Identity vetting
  - Either the person has to show the ID card to a DARIAH trusted person, e.g. at a conference (simple DARIAH registration authority)
  - Or the person sends a copy of the ID card

Policy for Homeless IdP: Registration

- B) Part of the scientific community
  - The person has to show that she is doing research, even without being part of a research organization
  - This could be done by sending a list of publications or by a confirmation of a research project

Policy for Homeless IdP: Data update

- We also have to proove that the status has not changed
- Automated mail to the users
  - If they mails to research email adresses return with „user unknown“ we delete them all others stay in Homeless IdP
  - The users with commercial email adresses have to activly write back and state that they are still part of the scientific community

DARIAH-EU

DAASI International

Data Protection Code of Conduct

- We want to support CoC
- We are part of the CoC uptake activity
  - DARIAH has already signed the support letter
  - Yes this makes the SP registration even more urgent

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

Thank you for listening!

Questions?

Comments?

Statements?