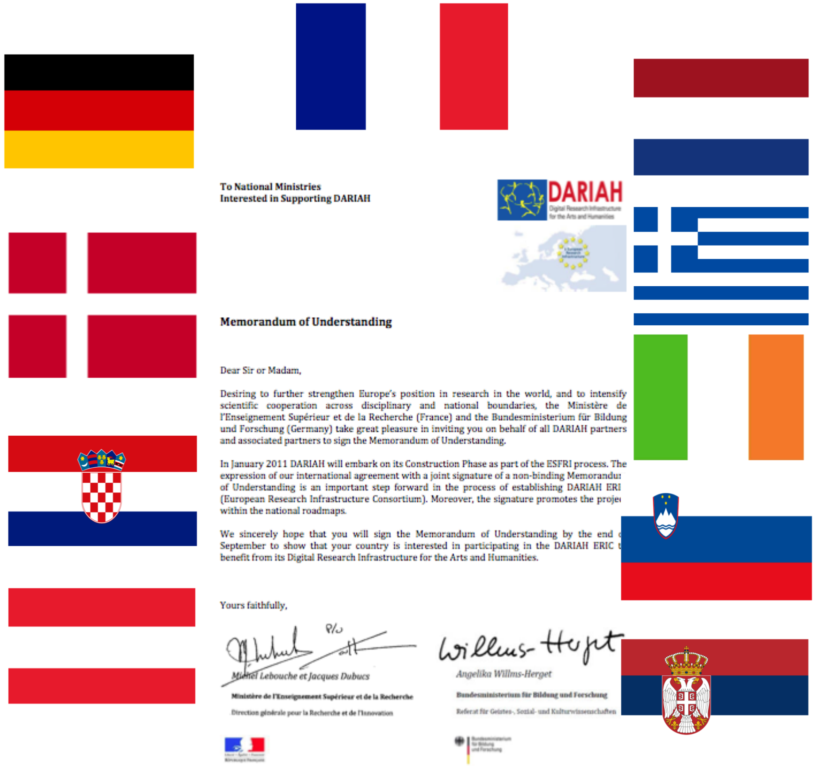
DARIAH- Update

6th FIM4R Workshop
Helsinki, October 2, 2013



To National Ministries
Interested in Supporting DARIAH

DARIAH
Digital Research Infrastructure for the Arts and Humanities

Memorandum of Understanding

Dear Sir or Madam,

Desiring to further strengthen Europe's position in research in the world, and to intensify scientific cooperation across disciplinary and national boundaries, the Ministère de l'Enseignement Supérieur et de la Recherche (France) and the Bundesministerium für Bildung und Forschung (Germany) take great pleasure in inviting you on behalf of all DARIAH partners and associated partners to sign the Memorandum of Understanding.

In January 2011 DARIAH will embark on its Construction Phase as part of the ESFRI process. The expression of our international agreement with a joint signature of a non-binding Memorandu of Understanding is an important step forward in the process of establishing DARIAH ERI (European Research Infrastructure Consortium). Moreover, the signature promotes the proje within the national roadmaps.

We sincerely hope that you will sign the Memorandum of Understanding by the end o September to show that your country is interested in participating in the DARIAH ERIC t benefit from its Digital Research Infrastructure for the Arts and Humanities.

Yours faithfully,

Michel Lebouche et Jacques Dubucs
Ministère de l'Enseignement Supérieur et de la Recherche
Direction générale pour la Recherche et de l'Innovation

Angelika Willms-Herget
Bundesministerium für Bildung und Forschung
Referat für Geistes-, Sozial- und Kulturwissenschaften

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

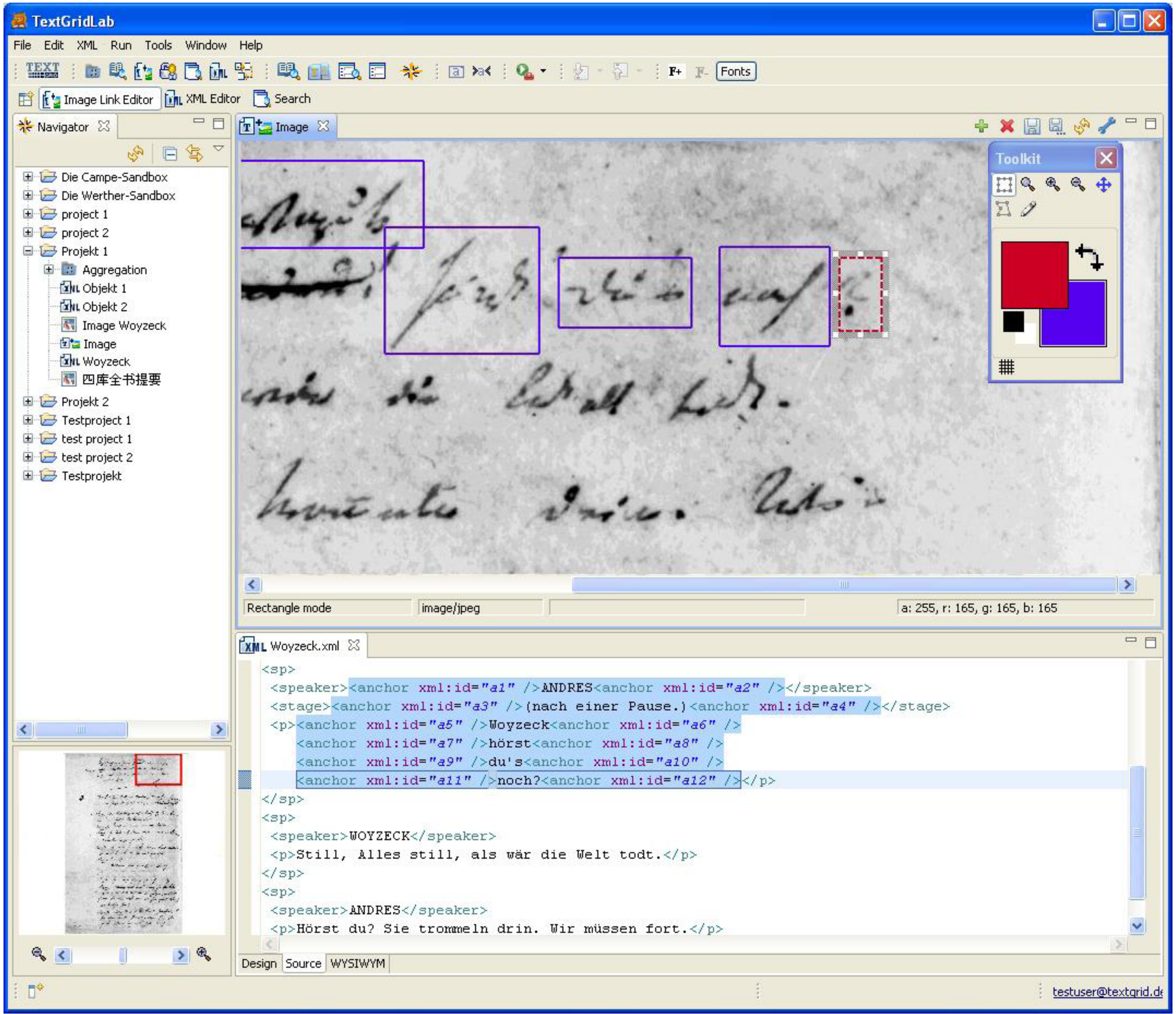
Infrastructure is administration, software and storage services but also Curricula and Methodology

Working with communities of practice: humanities scholars supporting their VREs

DARIAH-EU

DAASI International

Humanities VRE



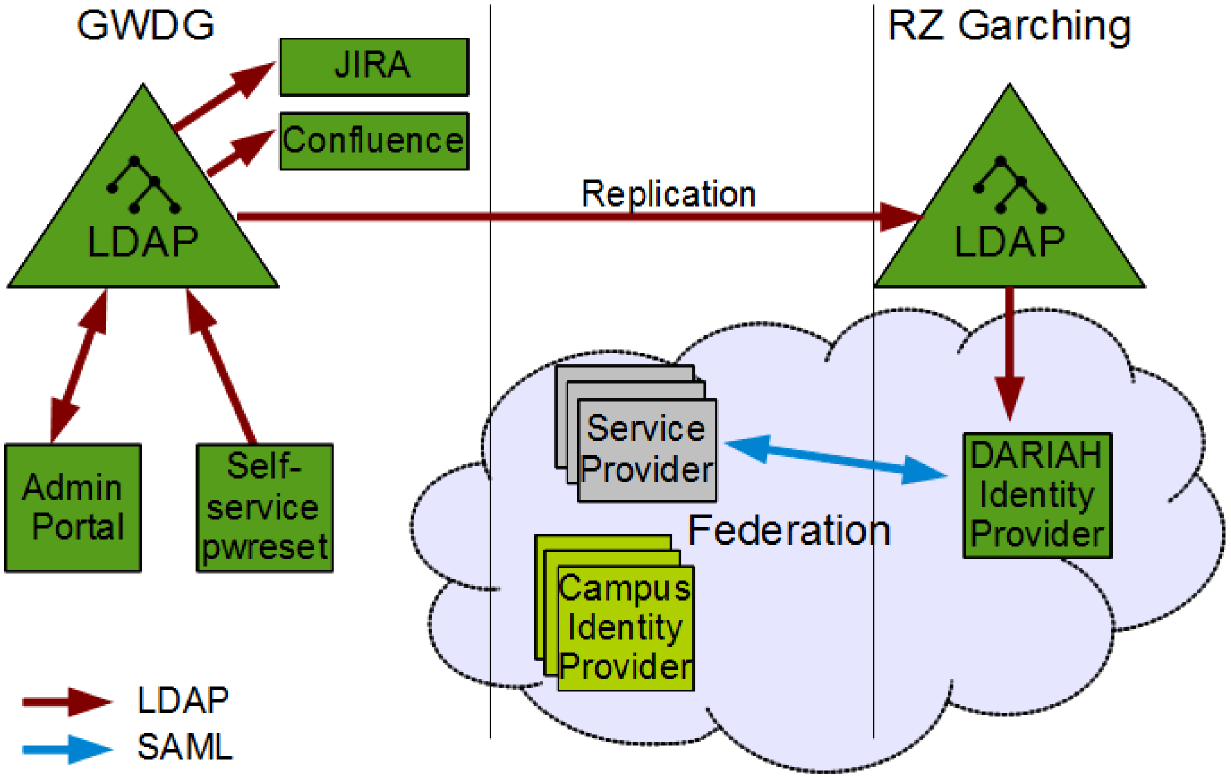
```
<sp>
 <speaker><anchor xml:id="a1" />ANDRES<anchor xml:id="a2" /></speaker>
 <stage><anchor xml:id="a3" />(nach einer Pause.)<anchor xml:id="a4" /></stage>
 <p><anchor xml:id="a5" />Woyzeck<anchor xml:id="a6" />
    <anchor xml:id="a7" />hörst<anchor xml:id="a8" />
    <anchor xml:id="a9" />du's<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 AAI Practice

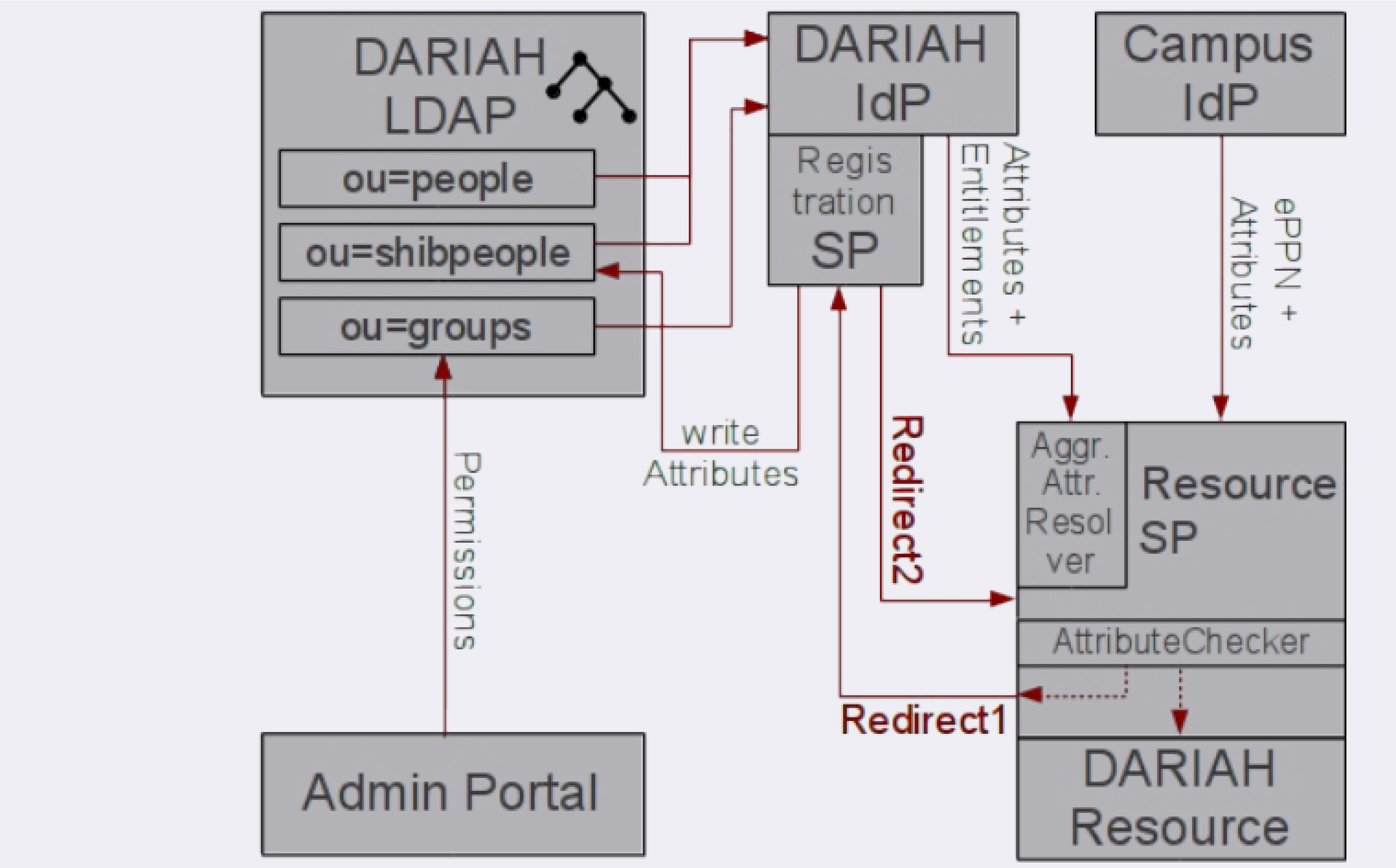
Current AAI set-up: a first version of an AA infrastructure has been deployed, based on two standards:

- 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

Current Set-Up



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?

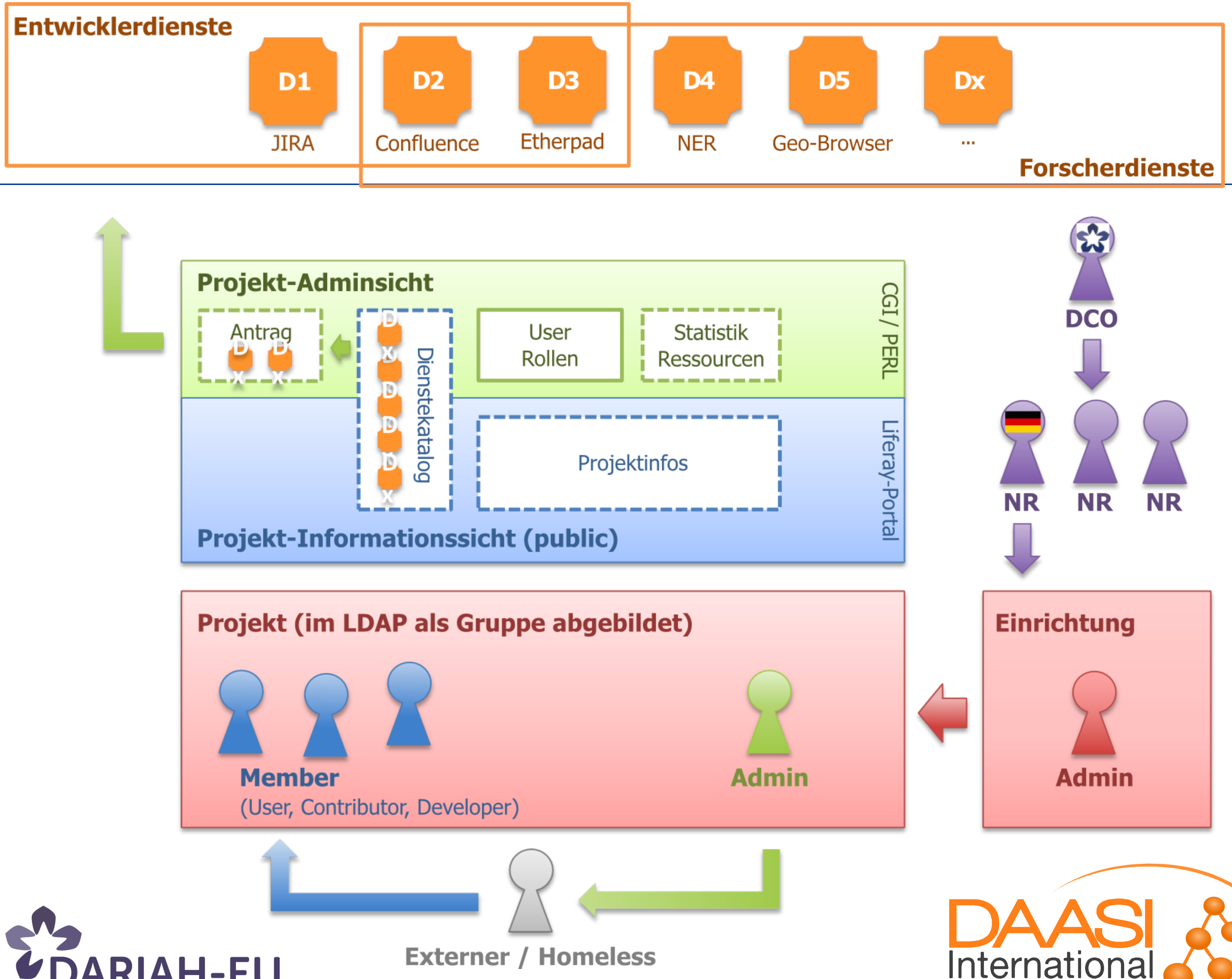
- We have productive a 'flat' Group based Authorization:
  - You are member of group
    - EHRI-users allowes to access the EHRI part of the DARIAH wiki
    - collection-registry-users allowes to use the collection registry
    - collection-registry-editors allowes to input data into the registry
    - 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

DARIAH-EU

DAASI International

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:

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

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

There will be a Humanities federation Workshop with DASISH partners to decide on this in October 17/18 in Cologne

DARIAH-EU

DAASI International

Thank you for listening

Is there time for questions?

DARIAH-EU

DAASI International

Further technical Plans

- It is planned to include technologies like OAuth2 and OpenID Connect into the DARIAH SAML based infrastructure
  - It is possible to have a SAML based Authentication within an OAuth-Infrastructure

as well as

  - To have an OpenID based authentication in a SAML based infrastructure.
- Experiments on these technologies have been performed successfully
- Main aim is that an application developer only has to support one API for AAI.

DARIAH-EU

DAASI International

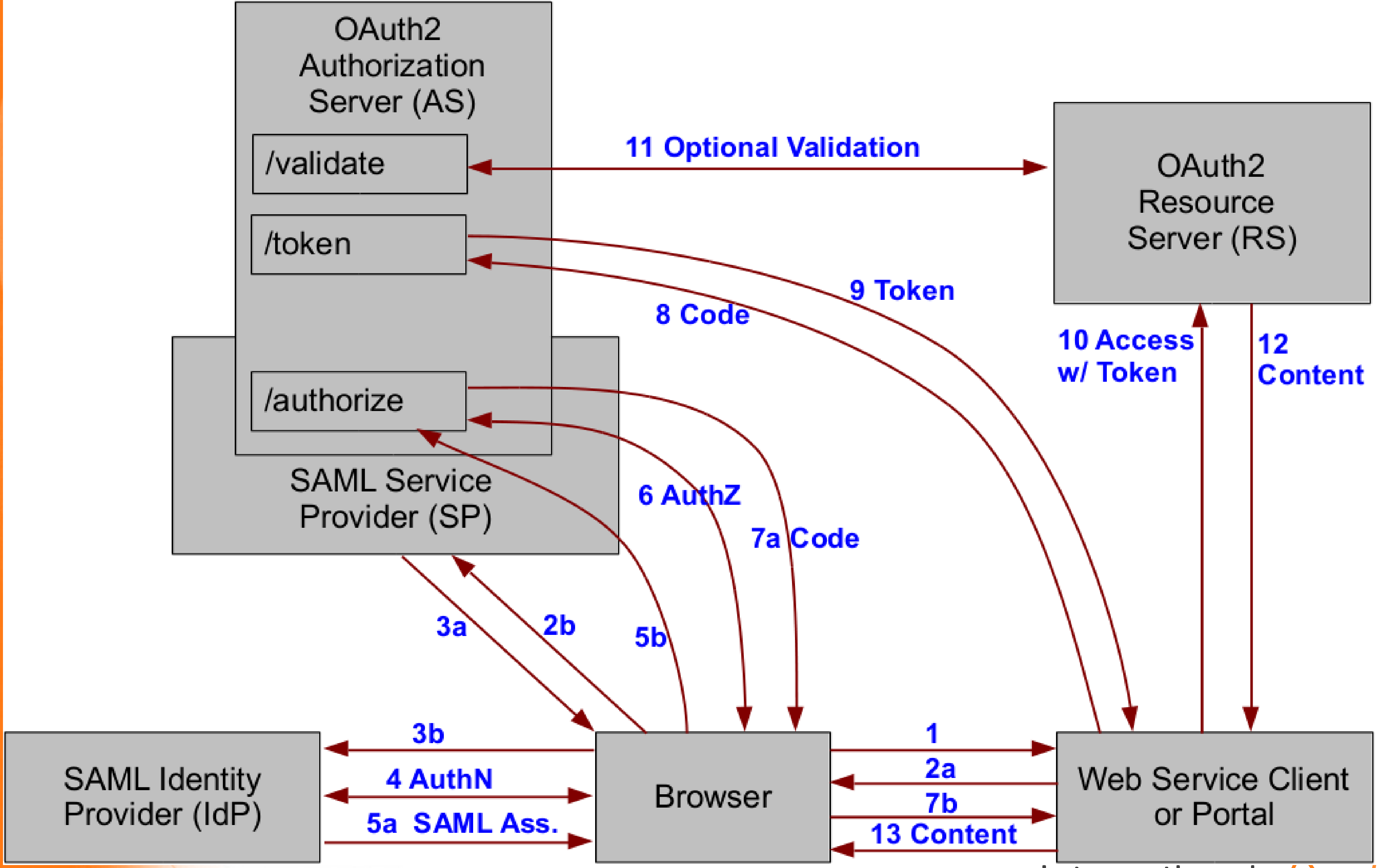
Web Services

- Adoption of ECP both in SPs and clients low
- Consideration of OAuth2
  - Simpler implementation for clients, pure HTTP(S) and JSON
  - Authorization Server could be shared for multiple resource servers → presumably less implementation effort on the resource side
  - Allows for 1-tier delegation
  - SAML IdPs can be connected via SAML Bearer Token
  - Access and Refresh Token instead of login/password
  - Natively uses OpenID Connect for AuthN (and other mechanisms possible, instead of SAML, if needed)
- OAuth2 standard pushed by the industry, so probably better bet in the future?

Web Services and Delegation: OAuth2

- New IETF Standard OAuth2 provides both for
  - delegation (1-Hop, not N-Tier) and
  - simple RESTful clients API (compared to ECP)
- OAuth2 is an Authorization Protocol, and leaves the Authentication method open
- Token-based mechanism:
  - one-time authorization code
  - access token
  - refresh token
- Can be integrated in a SAML federation using the OAuth2 SAML Bearer Profile
- Simply by protecting the OAuth2 Authorization Server's /authorize endpoint by a SAML SP within the federation

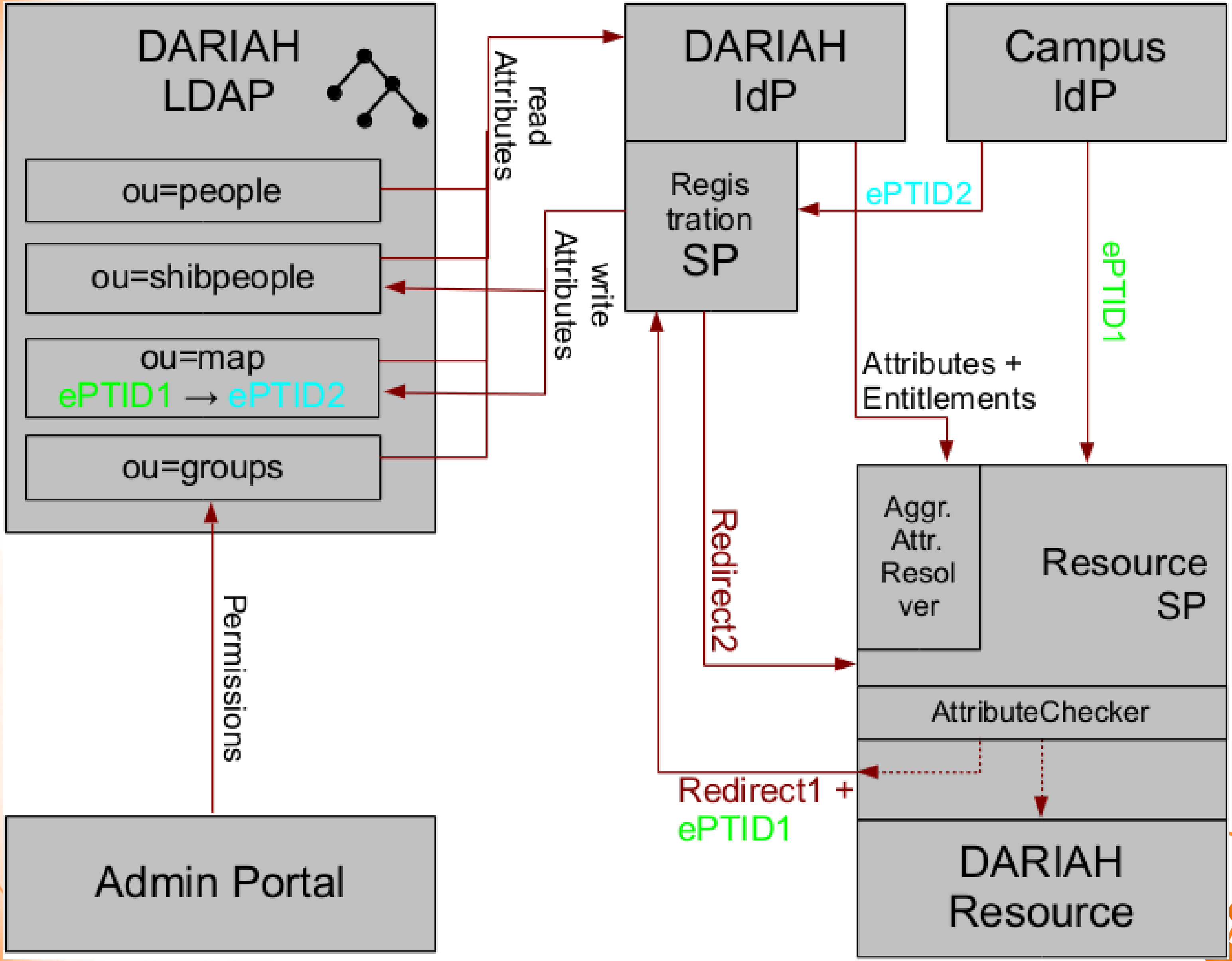
OAuth2 AuthZ Code Flow with SAML



IdPs that do not release ePPN

- Due to data protection and privacy issues, some IdP maintainers decide to only release a pseudonymous ID that is
  - cryptic
  - unique for that particular user and SP combination
  - e.g. eduPersonTargetedID (ePTID) or persistentID
- We have a solution where user self-asserts any attribute at the DARIAH registration SP
- Use a mapping table
  - SP1' ID1 maps to Registration SP IDX
  - SP2' ID2 maps to Registration SP IDX as well
  - When SP2 sends an Attribute Query for ID2, IdP maps ID2 to IDX, where all user attributes can be found
- This is work in progress!

IdPs that do not release ePPN


DARIAH LDAP
ou=people
ou=shibpeople
ou=map
ePTID1 → ePTID2
ou=groups
read Attributes
write Attributes
DARIAH IdP
Campus IdP
Regis tration SP
ePTID2
ePTID1
Attributes + Entitlements
Redirect2
Aggr. Attr. Resol ver
Resource SP
AttributeChecker
Redirect1 + ePTID1
DARIAH Resource
Permissions
Admin Portal