Gestaltung eines Antrags- und Berechtigungs-Workflow

Berechtigungsmanagement mit didmos LUI am Beispiel der Projekte TextGrid und DARIAH

ZKI AK Verzeichnisdienste, Chemnitz
16.-17.3. 2017

Peter Gietz, DAASI International

DAASI International

Inhalt

- LDAP als Datenbanktechnologie
- Berechtigungsmanagement ganz sicher
- Usecase TextGrid und DARIAH
- didmos
- Berechtigungs management mit didmos LUI

DAASI International

LDAP als Datenbanktechnologie

Wozu LDAP

- Ursprünglich wurde LDAP (als es noch X.500 hieß) definiert um ein weltweit verteiltes elektronisches Telefonbuch (white pages und yellow pages) zu implementieren
- Hierfür wurde eine objektorientierte Datenbank konzipiert und Objekte für diesen Use-Case spezifiziert (X.520 und X.521, vgl RFC 2256):
  - Top, alias, country, locality, organization, organizationalUnit, person, organizationalPerson, organizationalRole, groupOfNames, resitentialPerson
- Aber auch andere Dinge:
  - ApplicationProcess, applicationEntity, dSA, device

DAASI International

Wozu LDAP

- Dann hat man sich Gedanken gemacht über sicherere Authentifizierungsverfahren als Passwort und X.509 wurde geboren, das sich dann verselbstständigt hat:
  - strongAuthenticationUser, certificationAuthority, userSecurityInformation, certificationAuthority-V2, cRLDistributionPoint …
- Kurz nachdem 1988 X.500 standardisiert wurde, gab es erste Pilotprojekte in USA und UK, und man sah, dass es noch viele weitere praktische Informationen im X.500-Directory geben könnte

DAASI International

Wozu LDAP

- RFC 1274: Barker und Kille:
  - Directory Services are a fundamental requirement of both human and computer communications' systems. Human users need to be able to look up various details about other people: for example, telephone numbers, facsimile numbers and paper mail addresses. ***Computing systems also need Directory Services for several purposes: for example, to support address look-ups for a variety of services, and to support user-friendly naming and distribution lists in electronic mail systems.***

DAASI International

Wozu LDAP

- RFC 1274: Barker und Kille:
  - Deswegen wurde sowohl ein Verfahren spezifiziert, wie neues Schema in den Standard aufgenommen werden kann sowie die Objekte, die in den Piloten benötigt wurden:

```
pilotObject OBJECT-CLASS
        SUBCLASS OF top
        MAY CONTAIN {
            info,
            photo,
            manager,
            uniqueIdentifier,
            lastModifiedTime,
            lastModifiedBy,
            dITRedirect,
            audio}
    ::= {pilotObjectClass 3}
```

DAASI International

Wozu LDAP

- RFC 1274: Barker und Kille:

```
pilotPerson OBJECT-CLASS
        SUBCLASS OF person
        MAY CONTAIN {
                userid,
                textEncodedORAddress,
                rfc822Mailbox,
                favouriteDrink,
                roomNumber,
                userClass,
                homeTelephoneNumber,
                homePostalAddress,
                secretary,
                personalTitle,
                preferredDeliveryMethod,
                businessCategory,
                janetMailbox,
                otherMailbox,
                mobileTelephoneNumber
                pagerTelephoneNumber,
                organizationalStatus,
                mailPreferenceOption,
                personalSignature}
        ::= {pilotObjectClass 4}
```

Wozu LDAP

- RFC 1274: Barker und Kille: weitere Objektklassen:
  - account
  - document
  - documentSeries
  - room
  - domain
  - rFC822localPart
  - dNSDomain
  - domainRelatedObject
  - friendlyCountry
  - simpleSecurityObject
  - pilotDSA
  - qualityLabelledData

DAASI International

Wozu LDAP

- Mittlerweile hat sich LDAP als Authentifizierungsserver etabliert, aber aus den Ursprüngen können wir lernen:
  - LDAP eignet sich für beliebige Daten, die über das Netz (über ein standardisiertes Protokoll) zur Verfügung stehen sollen
  - Man kann eigene Klassen und Attribute spezifizieren und, wenn diese von mehreren Anwendungen genutzt werden sollen auch standardisieren
  - Dabei bekommt man alle Vorteile von LDAP (Skalierbarkeit, schnelle Lesezugriffe, sichere Authentifizierungsverfahren, etc.) umsonst dazu

DAASI International

Berechtigungsmanagement ganz sicher

Berechtigungsmanagement

- LDAP wird nicht nur zur Authentifizierung, sondern auch zur Autorisierung verwendet (als Metadirectory auch noch zu vielem mehr)
  - Autorisierungsinformationen sind z.B.:
    - Gruppenmitgliedschaften
    - Rollenmitgliedschaften
    - Autorisierungsattribute im User-Eintrag, wie z.B. allowedServices
  - Es ist wichtig die Vergabe der Berechtigungen zu kontrollieren und zu protokollieren

DAASI International

Berechtigungsmanagement

- In einem größeren Projekt wird ein zentraler Verzeichnisdienst aus > 70 Active Directories gespeist und im Verzeichnisdienst Berechtigungsattribute gepflegt, die den Zugriff auf alle Fachanwendungen steuern.
- Da es sich um hochsensible Dienste handelt, müssen Änderungen an den Berechtigungsattributen über einen Genehmigungs-Workflow geschützt werden
- Hierfür haben wir ein OpenLDAP-Overlay geschrieben, das angestoßen wird, wenn ein Berechtigungsattribut geschrieben werden soll. Das Overlay schreibt den Wert in ein Shadow-Attribut und stößt einen externen Workflow an. Nachdem zwei Genehmiger die Berechtigung bestätigt haben, sorgt der Workflow dafür, dass das Attribut endgültig ins LDAP geschrieben wird.

DAASI International

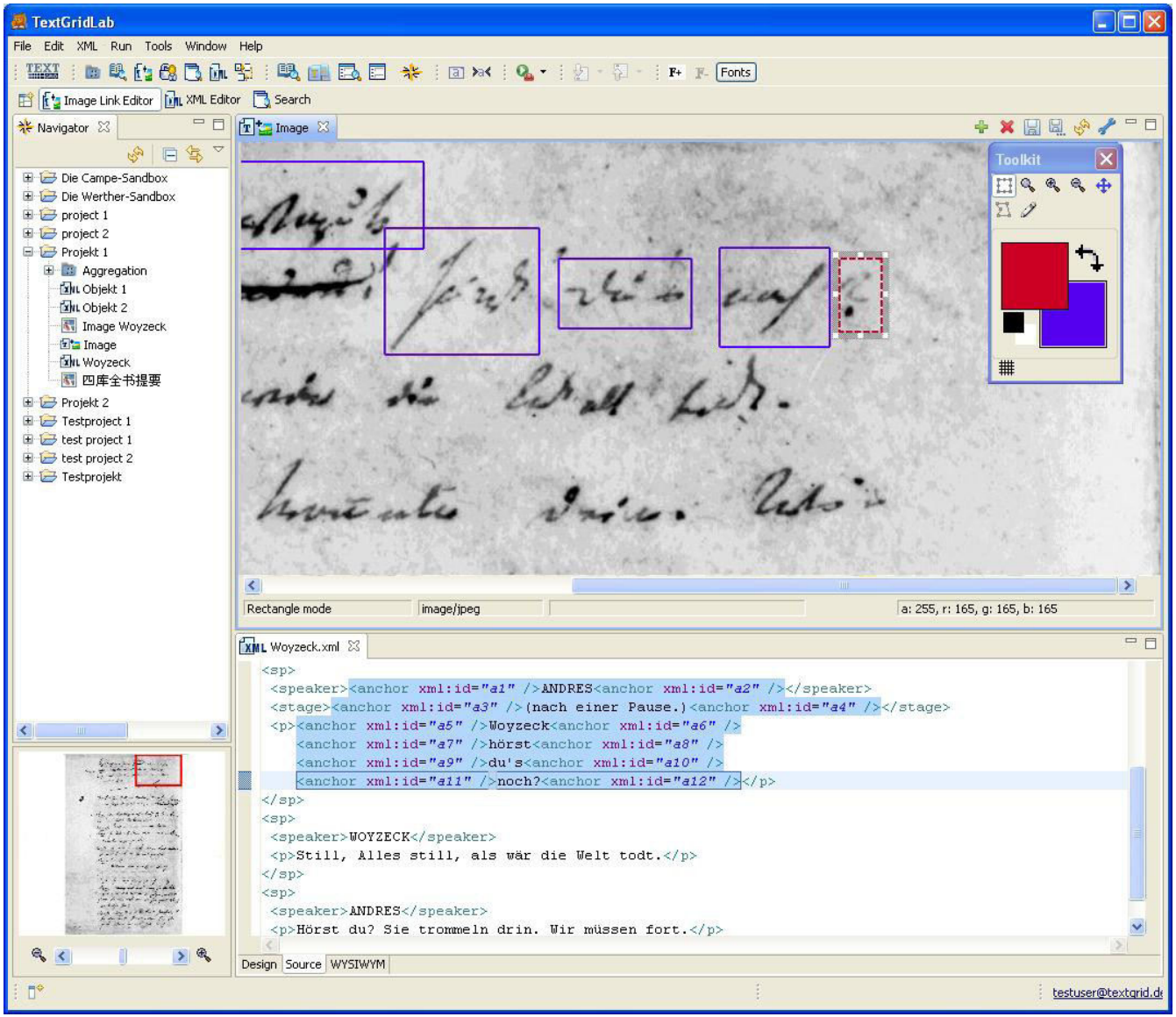
Usecase TextGrid und DARIAH

TextGrid

- Virtuelle Forschungsumgebung für textbasierte Geisteswissenschaften
- Mit Anbindung an einem Repository, in dem Dokumente abgelegt werden können, wobei projektspezifische Berechtigungen definiert werden können:
  - Projekt X
    - Projektrolle 1 (Darf nur lesend auf Projektdokumente zugreifen)
    - Projektrolle 2 (Darf schreibend zugreifen)
    - Projektrolle 3 (Darf Projektrollen zuweisen)

DAASI International

TextGrid



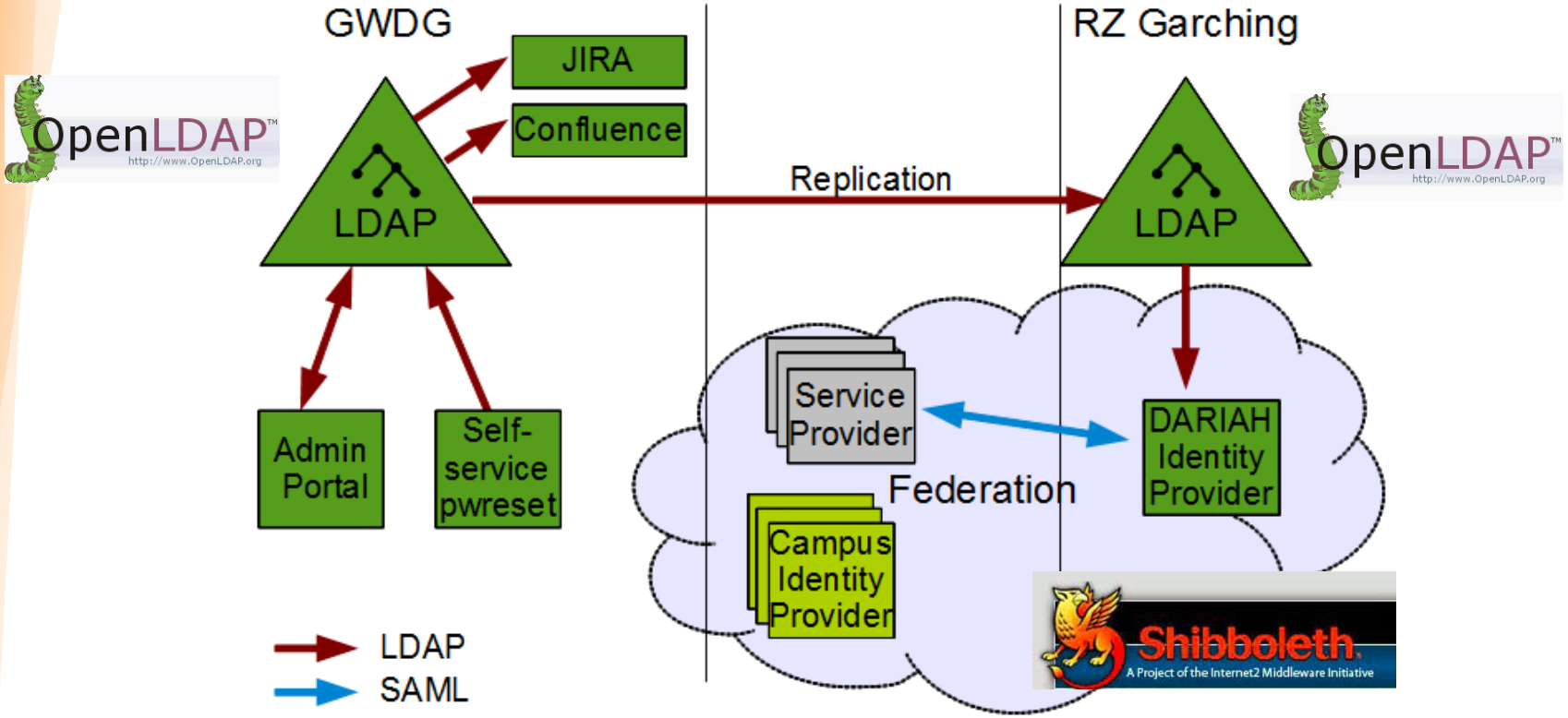
DAASI International

DARIAH

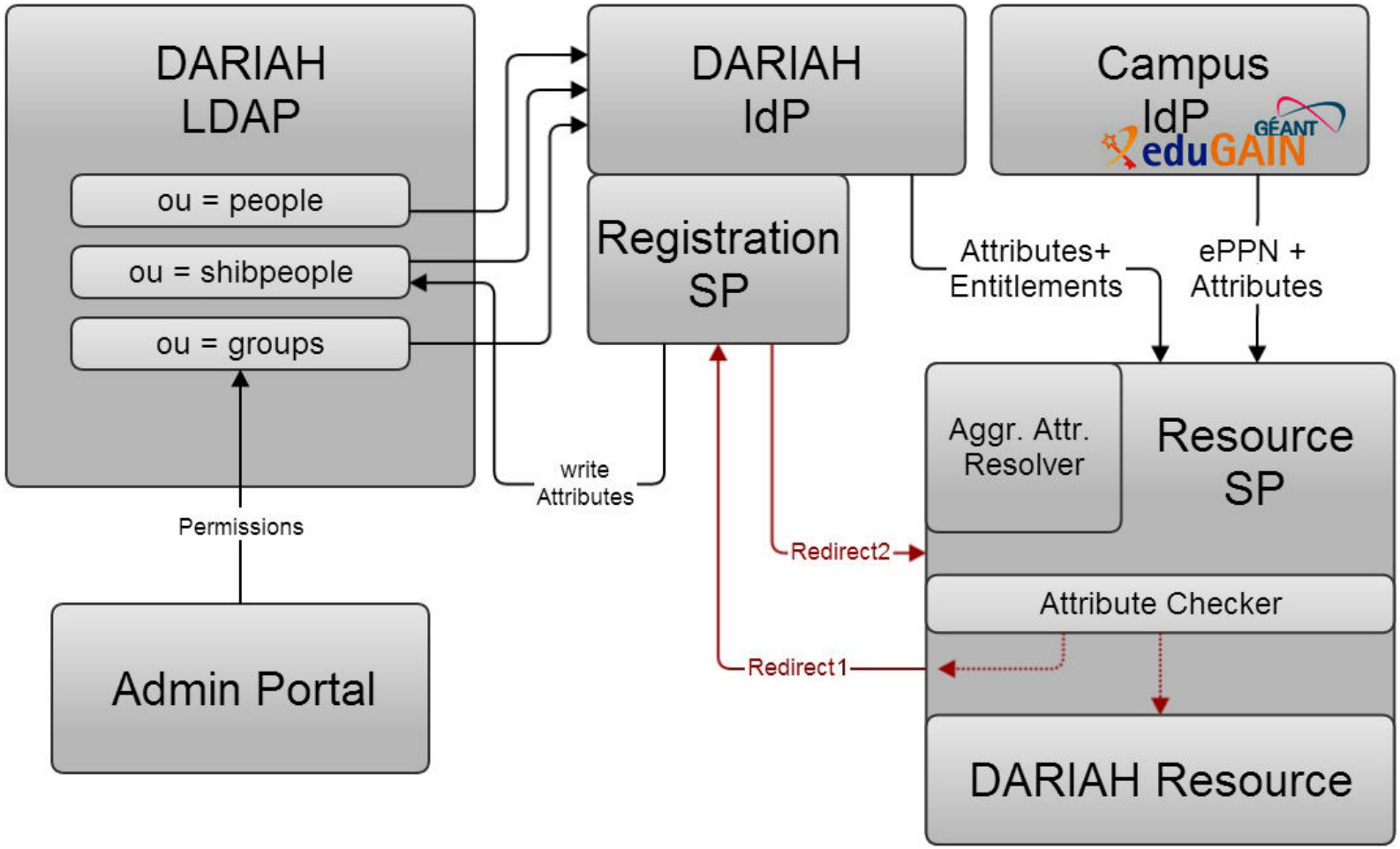
- Digital Research Infrastructure for the Arts and Humanities
- Ist eine Forschungsinfrastruktur für Geisteswissenschaften, die generische Dienste für Virtuelle Forschungsumgebungen bieten
- Bietet unter Anderm die DARIAH-AAI
- Die TextGrid-Benutzerverwaltung wurde in die DARIAH-AAI integriert

DAASI International

DARIAH-AAI


GWDG
RZ Garching
JIRA
Confluence
LDAP
Replication
LDAP
OpenLDAP
http://www.OpenLDAP.org
OpenLDAP
http://www.OpenLDAP.org
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


DARIAH LDAP
ou = people
ou = shibpeople
ou = groups
DARIAH IdP
Registration SP
Campus IdP
GÉANT
eduGAIN
Attributes+ Entitlements
ePPN + Attributes
Aggr. Attr. Resolver
Resource SP
write Attributes
Permissions
Redirect2
Attribute Checker
Redirect1
Admin Portal
DARIAH Resource

Berechtigungen in DARIAH

- Berechtigungen werden über zentral im DARIAH-LDAP gespeicherten Gruppen verwaltet
- Über ein Self-Service können Gruppenmitglieschaften beantragt werden
- Über ein Administrationstool können solche Anträge bewilligt werden

DAASI International

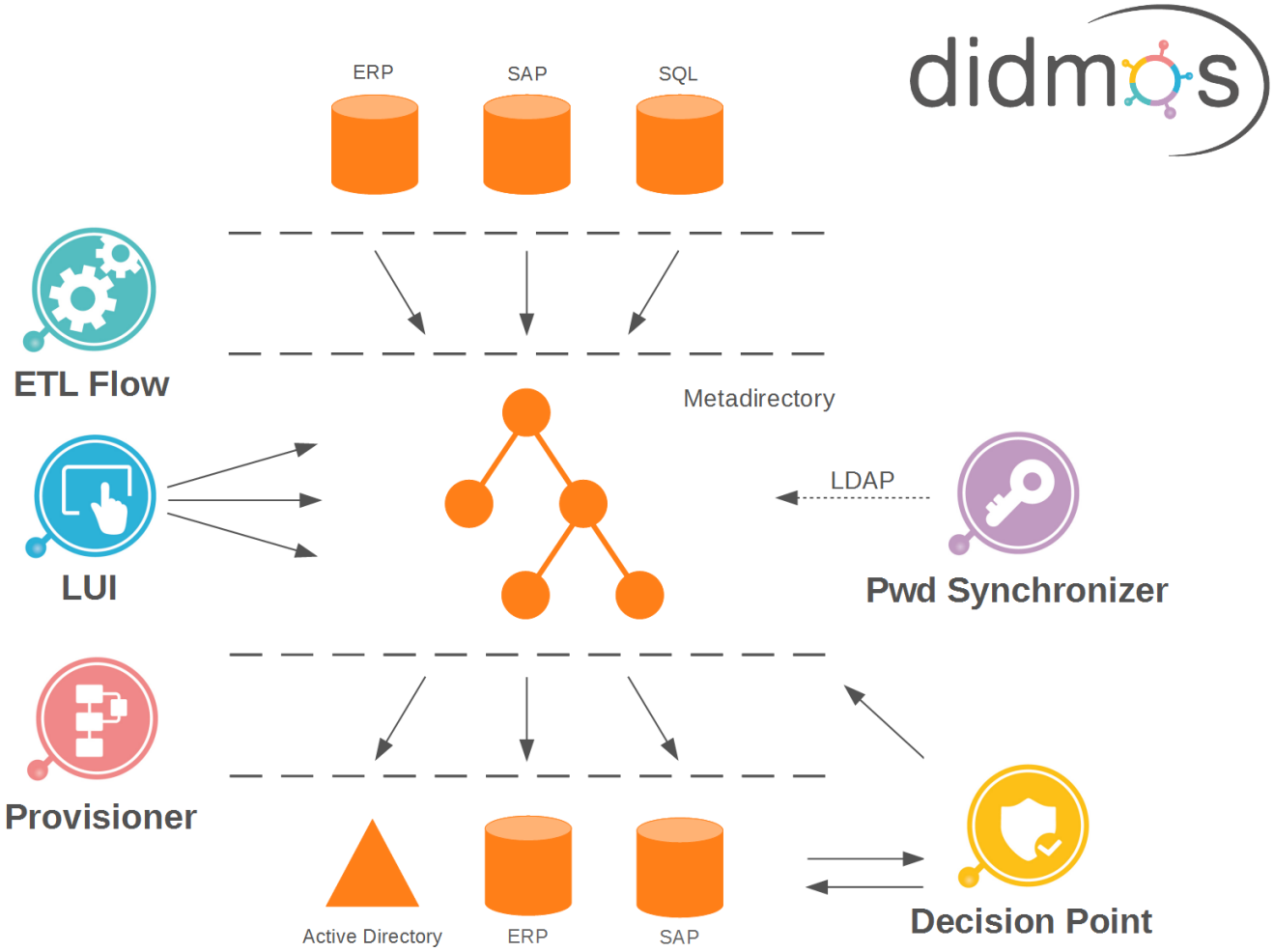
didmos

didmos

- DAASI Identity Management with Open Source
- Basiert auf OpenLDAP als Metadirectory
- Frameworkartig um flexibel alle Anforderungen erfüllen zu können
- Verwendet viel XML-Technologien, insb. XSLT, aber auch SAML, SPML, DSML, etc.
- Mit Didmos LUI (LDAP User Interface) können beliebige Frontends für Selfservice und für Administration von LDAP-Daten erstellt werden

DAASI International

didmos


didmos
ERP
SAP
SQL
ETL Flow
Metadirectory
LUI
LDAP
Pwd Synchronizer
Provisioner
Active Directory
ERP
SAP
Decision Point

Berechtigungs management mit didmos LUI

Berechtigungsworkflow mit didmos LUI

- Anträge für Accounts, Gruppenmitgliedschaften, Rollenmitgliedschaften, etc. etc. werden als LDAP-Objekte gespeichert
- Objektklasse lpRequest (didmos LUI hieß früher ldapportal = LP):

```
objectclass ( lpClasses:2
        NAME 'lpRequest'
        SUP top
        STRUCTURAL
        MAY ( lpRequestText $ lpRequestGranted $ lpRequestDecisionText $
              lpRequestType $ lpRequestDecisionFunction $ lpRequestData $
              lpRequestApplicant $ lpRequestDeciderDN $ lpRequestApplicantDN )
        MUST ( lpRequestNumber $ lpRequestTimestamp ) )
```

- Es ist möglich, projektspezifische Klassen, hiervon abzuleiten

DAASI International

Berechtigungsworkflow mit didmos LUI

- LpRequestNumber: eindeutige Nummer
- LpRequestText: Antragstext, den der User eingibt
- LpRequestGranted: Boolscher Schalter zunächst auf FALSE
- LpRequestDecisionText: Begründung des Genehmigers (muss bei Ablehnung ausgefüllt werden)
- LpRequestApplicant: Uid des Antragstellers
- LpRequestTimestamp: Zeitstempel des Antrags
- LpRequestDecisionFunction: Perl-Methode, die aufgerufen wird, nachdem eine Entscheidung getroffen wurde (z.B. addUserToGroup)
- LpRequestData: zusätzlich für die Methode benötigten Daten (z.B. GroupDN, Emailadresse zum Versenden von emails, etc.)

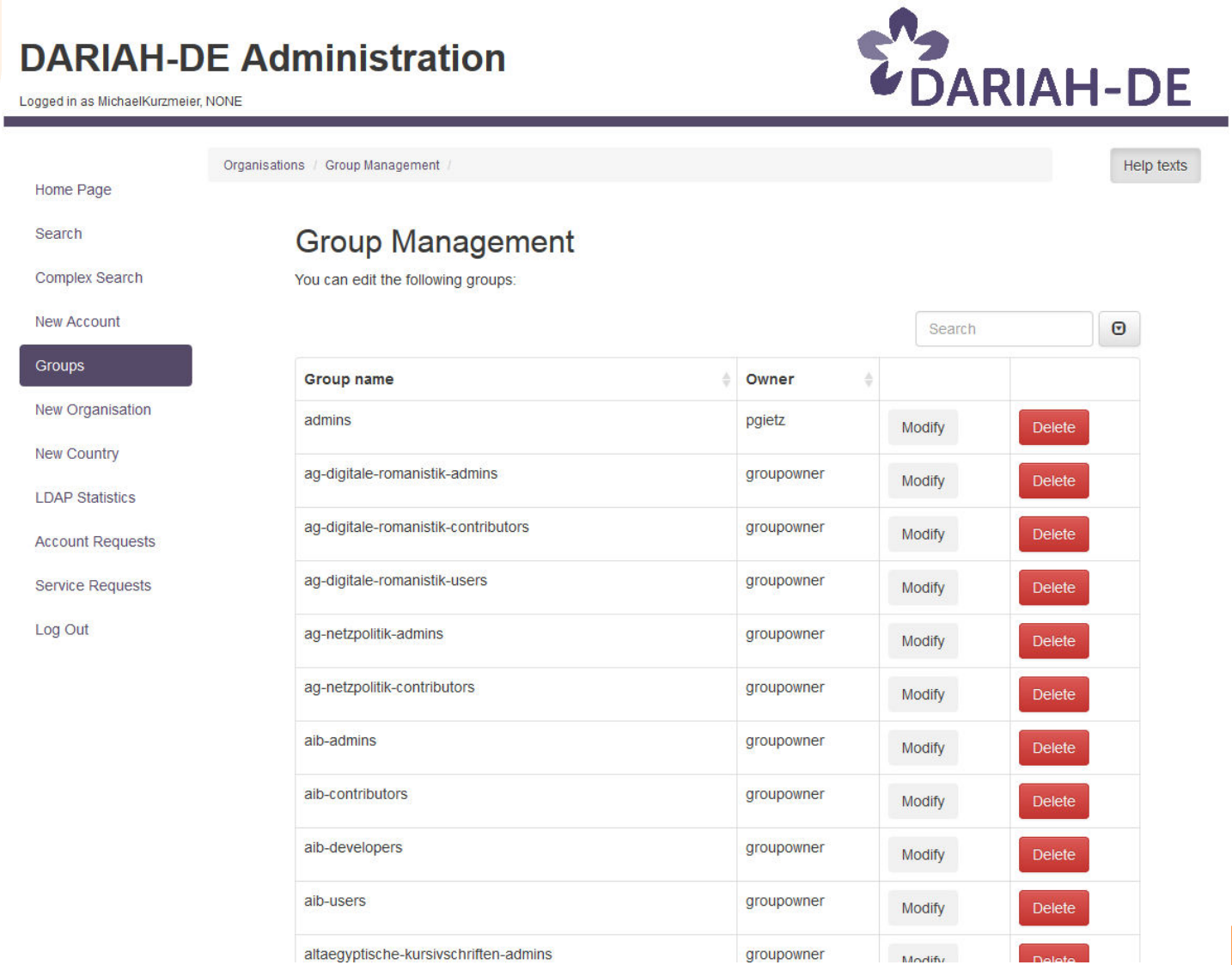
DAASI International

Berechtigungsworkflow mit didmos LUI

- Im Selfservice wird eine Maske zur Verfügung gestellt, in der ein Benutzer einen Antrag stellen kann
- Im Administrationstool, kann ein Administrator die Anträge anzeigen lassen, für die er (über Rollenzugehörigkeit) zuständig ist
- Er kann aus der Liste der Anträge über checkboxen die Auswählen, die er genehmigen möchte bzw. die die er ablehnen möchte und dann alle gleichzeitig genehmigen oder ablehnen (im letzteren Fall muss er dabei eine Begründung eingeben)
- In beiden Fällen erhält der User eine automatische E-Mail

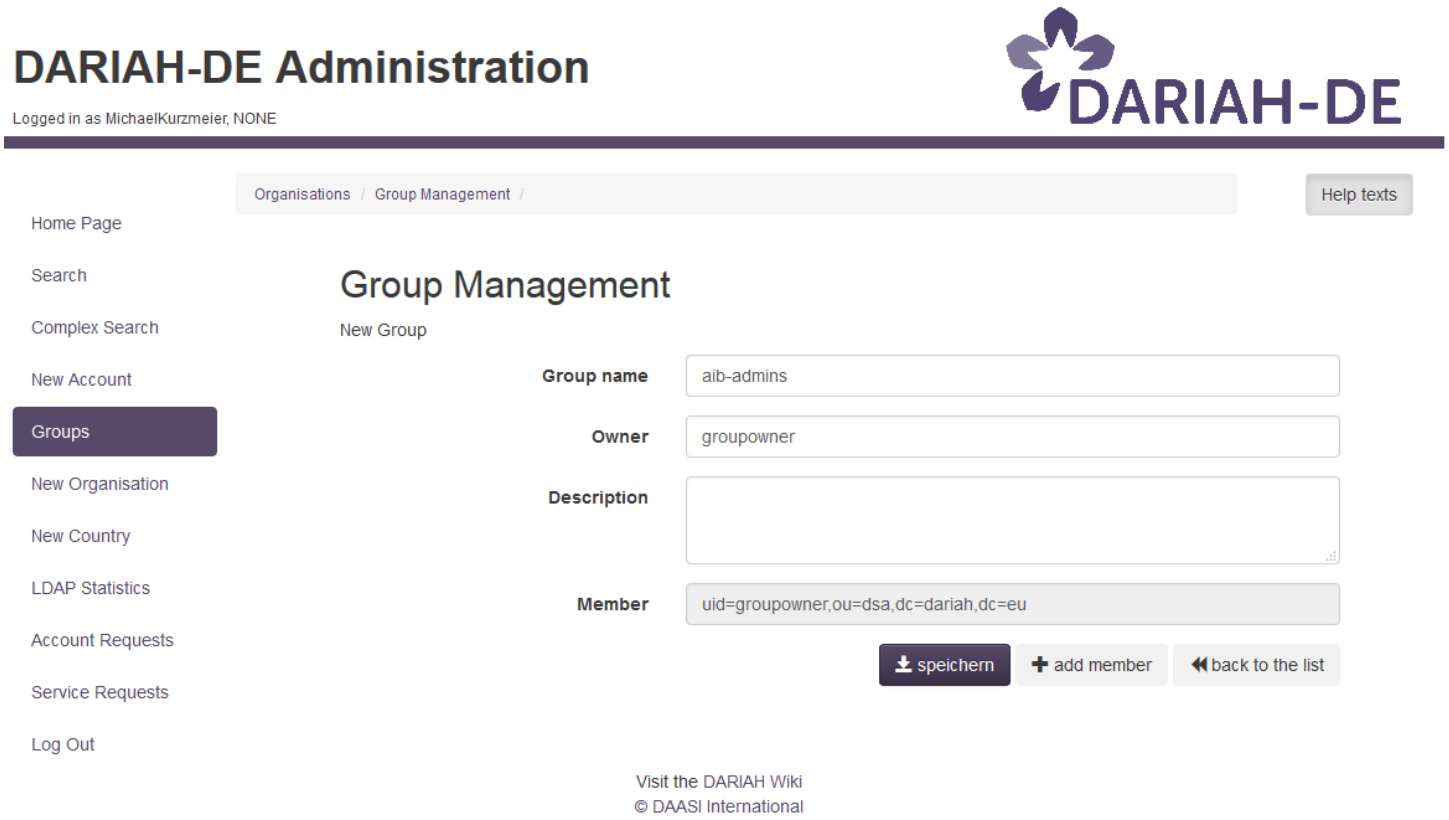
DAASI International

DARIAH Implementierung
Manuelle Gruppenzuordnung



DAASI International

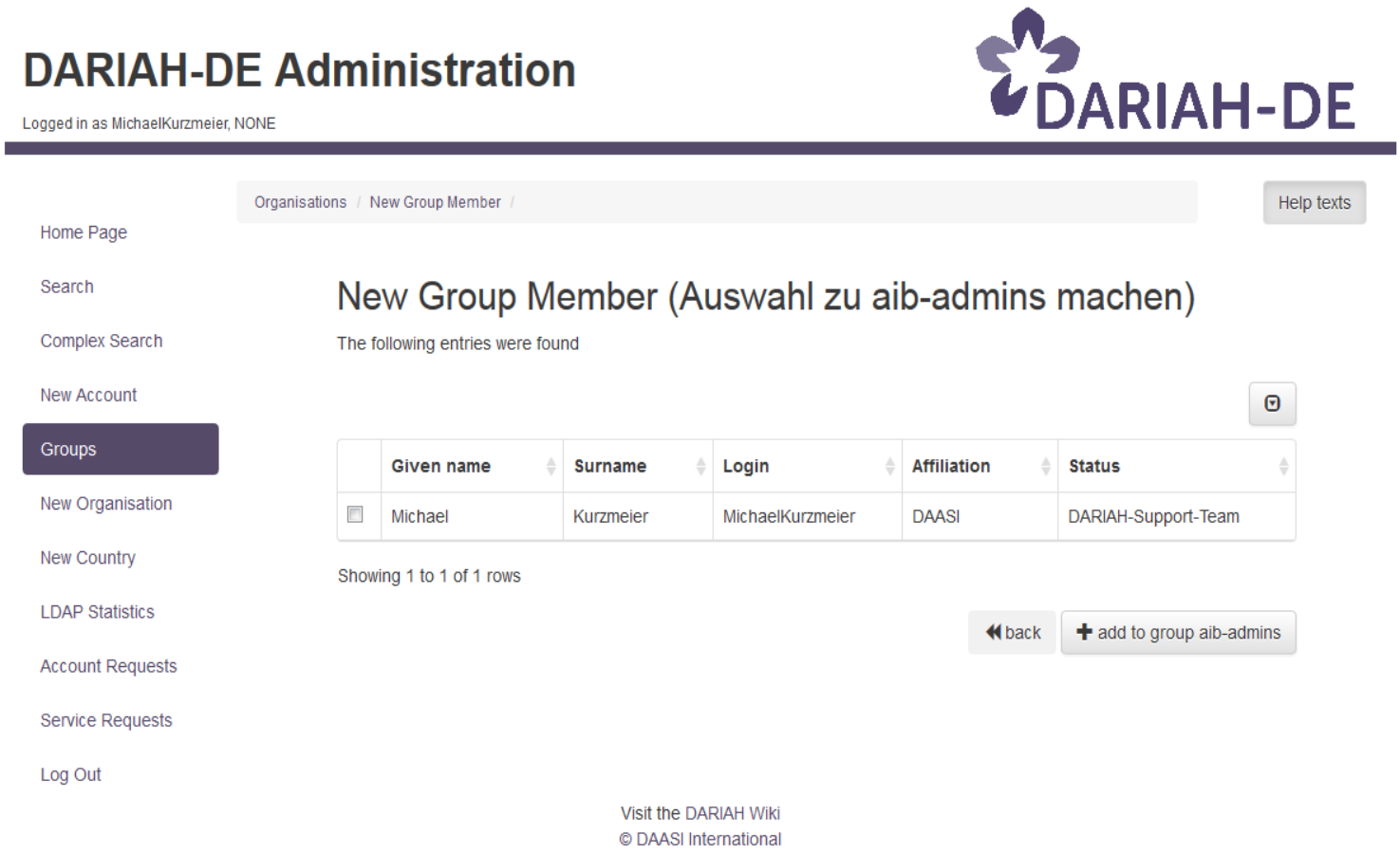
DARIAH Implementierung
Manuelle Gruppenzuordnung



DARIAH Implementierung
Manuelle Gruppenzuordnung

- XXX hier Suchmaske, die nach add member erscheint

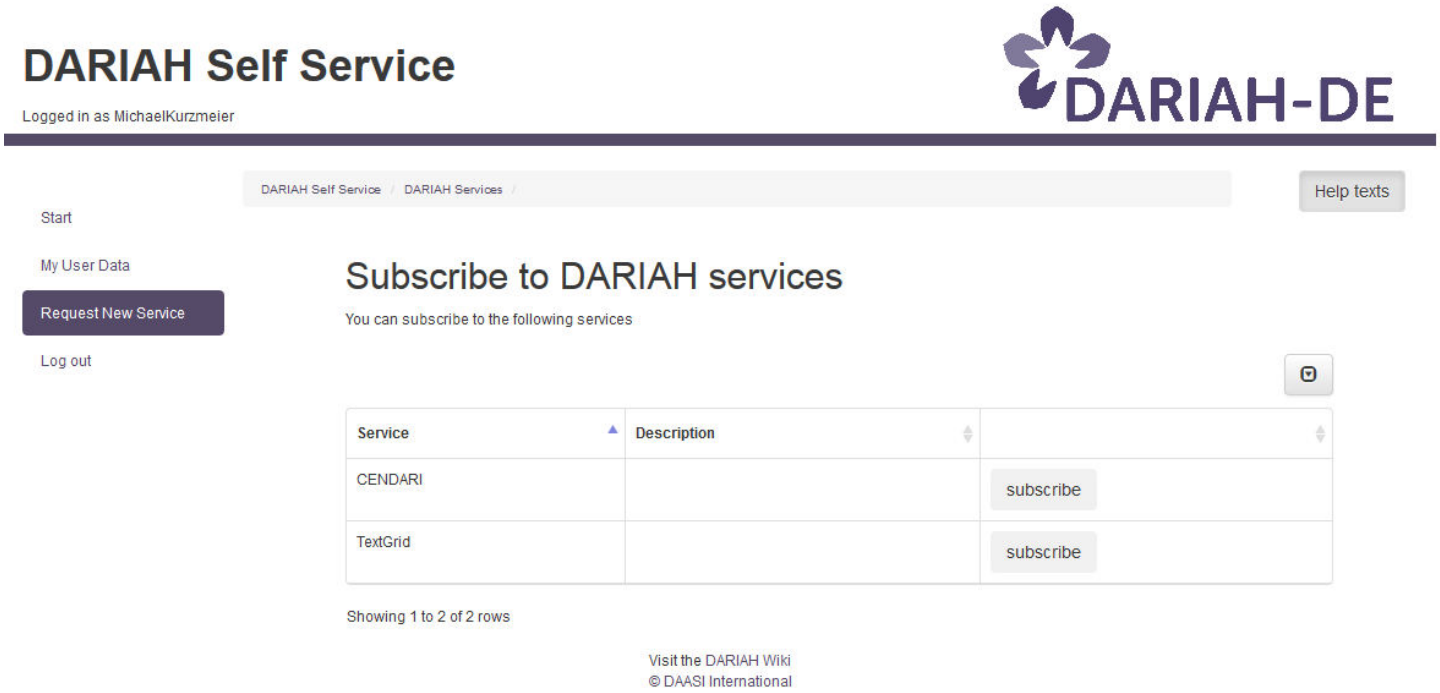
DARIAH Implementierung
Manuelle Gruppenzuordnung



DARIAH Implementierung
Manuelle Gruppenzuordnung

- Hier wieder Gruppe mit hinzugefgtem member

DARIAH Implementierung
Mit Antrags workflow



DARIAH Implementierung
Mit Antrags workflow

Dear __givenName__ __sn__,

your request for a DARIAH account has been received.
(request number __lpRequestNumber__ / __lpRequestTimestamp__)

The following basic data were provided by you:

Given name: __givenName__
Surname: __sn__
E-Mail: __mail__
Organisation: __o__

Initial Group
__member__

Remarks:
__lpRequestText__

You will receive an e-mail notification upon approval.

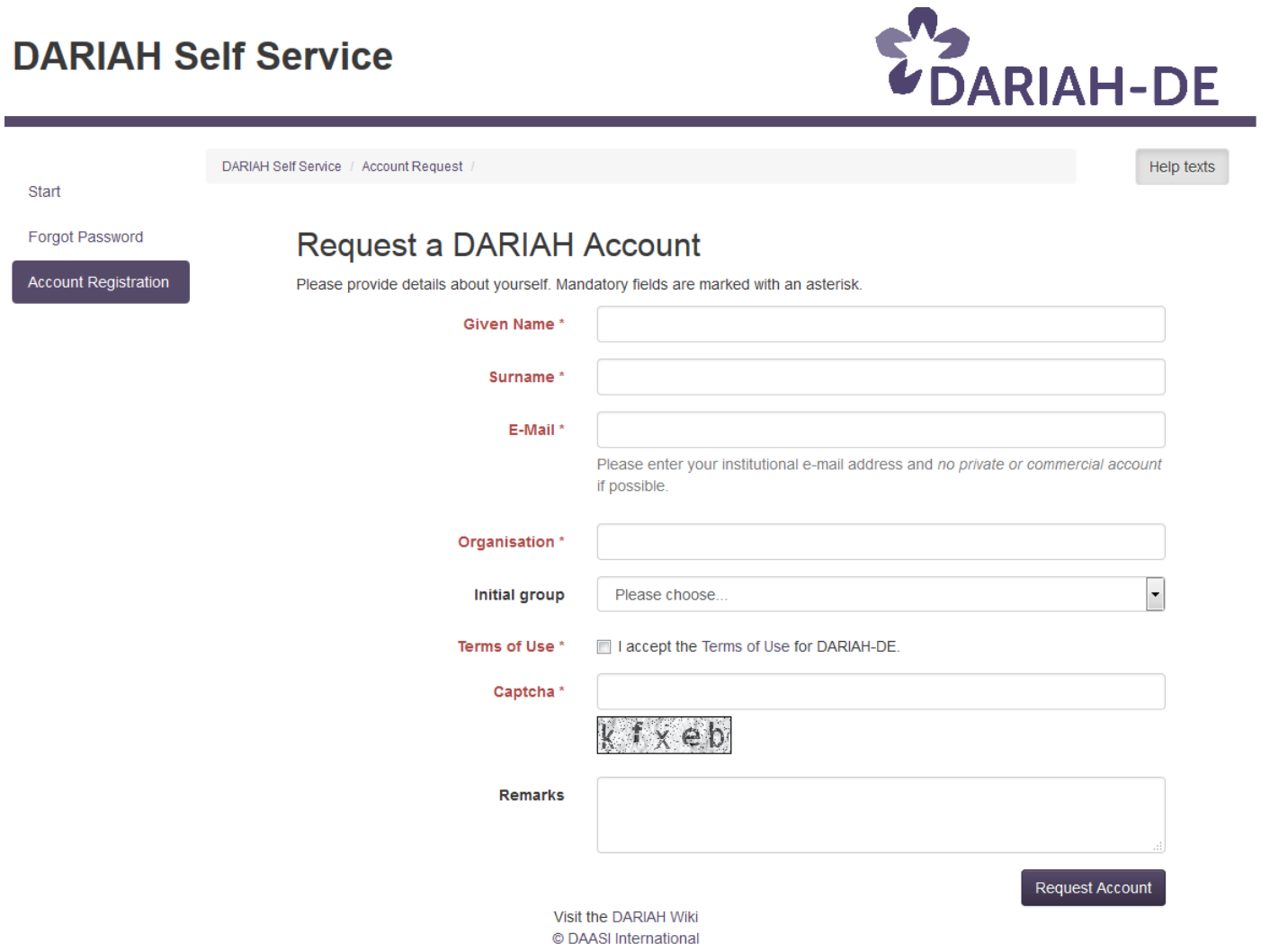
Best regards
DARIAH Administration

DAASI International

Mitgliedschaftsantrag genehmigen

- Hier eine Liste der Membershipanträge

Accountantrag



Antragsbestätigungsmail

Dear __givenName__ __sn__,

your request for a DARIAH account has been received.
(request number __lpRequestNumber__ / __lpRequestTimestamp__)

The following basic data were provided by you:

Given name: __givenName__
Surname: __sn__
E-Mail: __mail__
Organisation: __o__

Initial Group
__member__

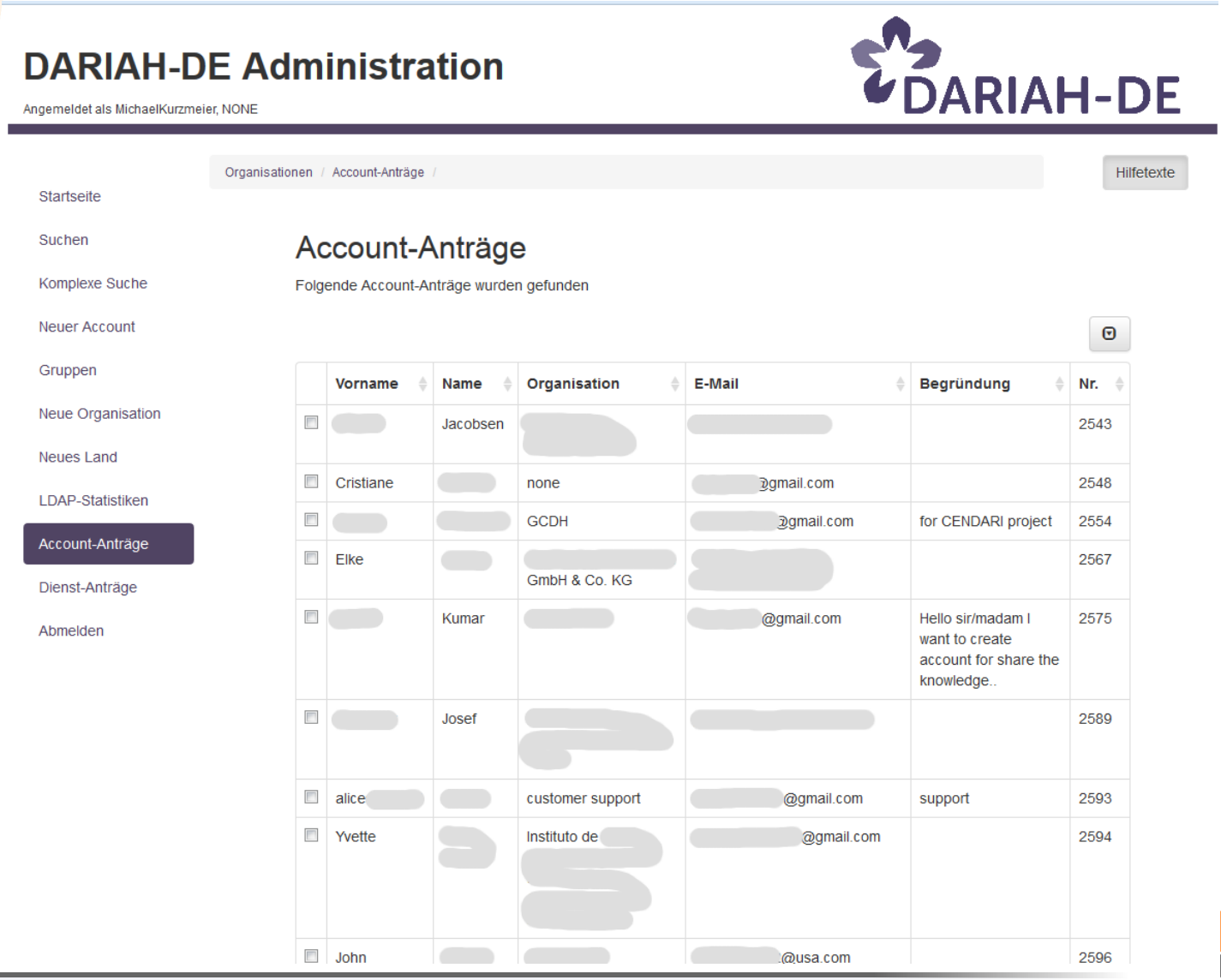
Remarks:
__lpRequestText__

You will receive an e-mail notification upon approval.

Best regards
DARIAH Administration

DAASI International

Accountanträge im Adminportal



Antragsgenehmigungsmail

Dear __givenname__ __surname__,

You had requested for a DARIAH account on __requesttime__.

Your account was __decision__ today.

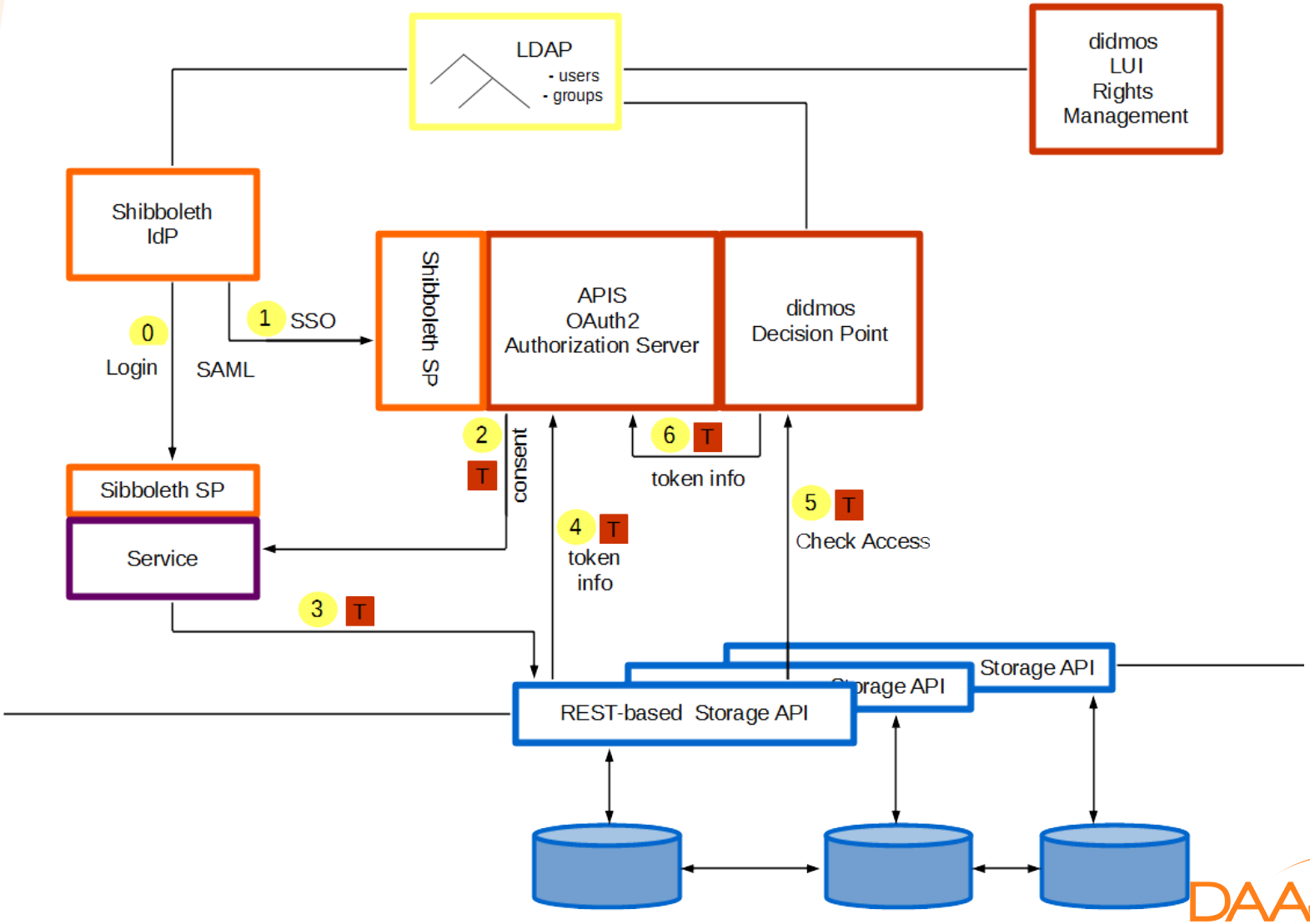
__decisionlabel__ __decisiontext__

__grantedRemark__

Best regards,

DARIAH Administration

DARIAH Policy Decision Point



Vielen Dank für Ihre Aufmerksamkeit.

DAASI International

www.daasi.de

Telefon: 07071 4071090

E-Mail: info@daasi.de