Agenda

- Introduction to AAI and current status in DARIAH (Peter)
- Demonstration of the administration tool for distributed rights management (Peter)
- Authentication/authorization process at Speech and Language Data Repository (Bernard)
- 2 or 3 very-very short (5 min) slots for last minute contributions (N.N.)
Agenda bashing

• Introduction round?
• Possible other themes:
  • EHRI AAI requirements
  • CENDARI AAI requirements
  • DASISH AAI Activities
  • DARIAH -NL -AT -XX AAI
AII requirements

• The AII service must be easy to use, ideally using their own institutional credentials (if available)
• Single sign-on to all (DARIAH) resources, tools and services in an idea world, researchers could use the same credential in any 'academic' context.
• Authorisation granularity
  • e.g. access to 'sensitive data': EHRI (European Holocaust Research Infrastructure)
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
How does a federation work?

• Setting the scene:
  • Users have a home organisation where they have a user account (Loginname/Password)
  • DARIAH has applications/services that users want to use and that need authentication and authorization

• A federation enables users to use their home account for authenticating at DARIAH services
How does a federation work?

- Three building blocks for a federation:
  - Identity Providers (IdP) that talk to the user's management system (where authentication is performed)
  - Service Providers, that protect applications sends the user to her IdP and receive assertions from that IdP
  - Federation management that knows which IdPs and which SPs belong to the federation and that establishes trust between them
How does a federation work?

- **SAML Assertions (the IdP gives to the SP):**
  - **Authentication assertions:**
    - The user you just sent to me was able to successfully authenticate (right now or a couple of hours ago)
  - **Attribute assertions:**
    - Additionally the user has a number of attributes, e.g.:
      - affiliation=faculty@copenhagen-university,
      - mail=john.doe@uni.copenhagen.dk
  - **Authorization assertion**
    - User is allowed to use Service X
    - Mostly not in use
SAML-Architecture

from: RUBENKING, NEIL J.: Securing web services
How does a federation work?

• Trusts:
  • Sps and IdPs trust the federation management that the list of SPs and IdPs is accurate
    - List contains only federation members
    - List consists of server certificates (for server authentication and encrypted communication)
  • SP trust the IdP that the assertions are correct
  • IdP trusts the SP that it will not do misuse of the personal data sent
Federation

IdP 1
IdP 2
SP 1
SP 2
...
IdP 2
SP 3
IdP 1
SP 2
SP 1
Authorization features

- 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 minimum 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
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)
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
How to make this a European-wide Infrastructure

- Develop and implement a hierarchical role model to delegate user rights management
- '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?
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
How to make this a European-wide Infrastructure

● Develop and implement a hierarchical role model to delegate user rights management
  • First prototype is ready and will be demonstrated now
● Additional functionality is on its way:
  • Webbased DARIAH 'homeless'-Account application
  • Webbased Group membership applications
  • Very easy application decision functionality in the administration tool
● So Software is sort of there, now how 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?
How to get the urgently needed European humanities federation?

- By now the demonstrated infrastructure is only accessibile via DFN-AAI or via a dedicated DARIAH ('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 Geant 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
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.
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?
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