ELIXIR and EGI Services Integration

Michal Procházka – Masaryk University
Slávek Licehammer - CESNET
Christos Kanellopoulos - GRNET
Nicolas Liampotis - GRNET
Outline

• Motivation
• EGI
• ELIXIR
• Proxy IdP/SP concept
• Joining two infrastructure
• Challenges
• Integrated applications
• Open issues
Motivation

• e-Infrastructures provide services for their users
• Sharing services lower the costs
• EGI as an e-Infrastructure providing computational and storage services for other e-Infrastructures
  • ELIXIR as a consumer of EGI services
• Users must be authenticated and authorized to use the services
EGI - European Grid Infrastructure

- EGI is a globally distributed ICT infrastructure which federates digital capabilities
- EGI AAI CheckIn service
  - User registration, account linking, supports federated access and SSO for EGI services
  - Currently GOCDB, AppDB, GGUS are integrated
  - X.509 based services connected via CILogon Token Translation Service
- EGI AAI is using Proxy IdP/SP concept
ELIXIR

• European infrastructure for biological information, supporting life science research and its translation to medicine, agriculture, bioindustries and society

• ELIXIR built an AAI infrastructure which provides unified access to all ELIXIR services

• The goal of ELIXIR AAI infrastructure is to provide similar access also for services which are outside the ELIXIR infrastructure provided by other research infrastructures like EGI

• ELIXIR AAI is using proxy IdP/SP concept
Proxy IdP/SP concept
Joining two infrastructures

- Separate accounts on both infrastructures - **NO**
- Register services in both infrastructures – **NO**

Solution: Join underlying AAI components

  Transparent for users and services

  Standards (SAML2)

  Utilization of existing services/infrastructures – identity federation, eduGAIN
How to provide services between e-Infrastructures?
Joining e-Infrastructures
Challenges

- Authorization
- Account linking
- WAYF/DS chaining
- Policies
Authorisation

- Use of eduPersonEntitlement attribute
  - missing widely accepted representation of entitlements
- Agreement on eduPersonEntitlement syntax and semantics
  - urn:mace:egi.eu:elixir-europe.org:member@vo.elixir-europe.org
- ELIXIR AAI releases information about user’s role understandable by EGI AAI
  - Virtual organization roles: VO administrator, VO member
Account linking

• ELIXIR issues ELIXIR ID for each user
  • Users can link their accounts to ELIXIR ID (institutional, social, ...)

• EGI issues EGI ID for each user as well
  • Users can link their accounts to EGI ID
  • Users who have both EGI and ELIXIR ID can link them as well

• ELIXIR users can access EGI services with their ELIXIR ID
WAYF/DS chaining
Policies

• Integration requires harmonization of policies and LoAs (AuthN, identity, attributes)

• ELIXIR AAI proxy IdP/SP can release personal data to EGI AAI due to
  • GÉANT Data Protection Code of Conduct (CoCo)
  • REFEDS Research and Scholarship (R&S)
Integrated applications

- GOCDB
  - Grid Configuration Database
  - Authentication
  - Authorization based on LoA (requires substantial or higher)

- AppDB
  - Application database of cloud virtual machines
  - Authentication
  - Authorization based on users’ roles
Open issues

- Standardisation of syntax and semantics of eduPersonEntitlement
- LoA harmonization on digital identities
  - LoA of authN method
  - LoA of identity vetting
  - LoA of user attribute values
- User experience - long way from user’s IdP to SP
  - Automate IdP selection
Conclusion

- ELIXIR-EGI integration was done closely with AARC project
  - http://aarc-project.eu
- Use of standards helped a lot
- Presented approach can serve as a reference for integration use cases
Thank you