ELIXIR AAI

Miroslav Ruda,
on behalf of  Mikael.Linden@csc.fi

European Life Sciences Infrastructure for Biological Information
www.elixir-europe.org
Use cases (Finished)
⇒ Requirements (stabile draft)
⇒ Design (first draft)
⇒ Technical Use Cases document
  – Prioritization with ELIXIR -EXCELRATE user groups
⇒ Small pilots in spring 2015
⇒ Deployment in ELIXIR Excelerate project
ELIXIR AAI design (draft)

ELIXIR AAI

- Credential translation
- ELIXIR Proxy IdP
- eduGAIN IdPs
- Common IdPs

ELIXIR Directory

Relying services

- EGA
- wiki
- Cloud
- Intranet
- Data archive

EGA
wiki
Cloud
Intranet
Data archive

Common IdPs

External authentication (e-infrastructures)

- Dataset authorisation management
- Group/role management
- Bona fide management
- Attribute self-management
Each user has one ELIXIR identity
- e.g. "tommi@elixir-europe.org"

ELIXIR Proxy maps external authentication providers to it
- e.g. nyronen@csc.fi (eduGAIN)
- e.g. tommioffinland@google (Google)
- e.g. 0000-0002-3634-3756 (ORCID)

Also local username/password possible

Credential translation

tommi@elixir-europe.org

nyronen@csc.fi tommioffinland@google

eduGAIN IdPs Common IdPs

Attribute self-management

External authentication (e-infrastructures)
Step-up authentication

Less sensitive services: password enough

Human data

wiki

ELIXIR Proxy IdP

Human data

tommi@elixir-europe.org

nyronen@csc.fi

tommioffinland@google

eduGAIN IdPs

More sensitive service: Step-up authentication server asks for second factor (e.g. one-time password by SMS)

External authentication: Authentication with password

ELIXIR AAI
Technical Use Cases

• Basic Technical Use Cases defined by AAI, Cloud and Data TFs

• Workshop in Amsterdam 12-13/3/15
  – 45 participants: Elixir, e-Infrastructure & Other Service Providers
  – Discuss requirements of the Scientific Use Cases

• Initial Prioritisation and Grouping Analysis
  – 0: Federated ID, Other ID
  – 1: Elixir ID
  – 2: Credential Translation, Group/Attribute Management, Endorsed Personal Data Attributes
AAI milestones in ELIXIR-Excelerate

EXCELERATE Milestone 4.1: (M12) Demonstrator I. Some ELIXIR Technical Services are operating and are usable to support aspects of the ELIXIR-Excelerate Use Cases.

- ELIXIR Identity established based on federated Identity
- Credential translation
- Bona fide researcher qualification management

EXCELERATE Milestone 4.2 (M24) Demonstrator II. Most ELIXIR Technical Services operating and in more robust and sustained manner and capable of supporting most aspects of the ELIXIR-Excelerate Use Cases.

- group/attribute management, endorsed attribute
- Other external Identity
Two pilots/use-cases

• Intranet usage – access to project documents, including group management
• Connect EGA archive to authorized Cloud services
  • Reliable and fast enough data transfer from archive to Cloud storage
  • Cloud authentication protocol uses ELIXIR AAI
  • Provide a secure protocol for Cloud users to access EGA datasets based on DAC permissions
  • Prototype Cloud VM data access rules that comply to EGA access regime.

Tools, dependencies

• EduGAIN IdPs + Google/ORCID
• ProxyIdP - SURF
• ELIXIR directory, group management - Perun
• DAC - REMS
• Several tools discussed for credential translation (SAML2 to X.509 certificates, Kerberos ...)

Pilot implementation