Case Studies in Federated Identity Management for Research Communities

Authors/Affiliations

Ann Harding, ann.harding@switch.ch +41 44 253 98 14 SWITCH/GN3plus
Peter Gietz, peter.gietz@daasi.de DAASI International GmbH/DARIAH
Tommi Nyrönen, tommi.nyronen@csc.fi CSC - IT Center for Science/ELIXIR
Mirjam van Daalen, mirjam.vandaalen@psi.ch, Paul Scherrer Institute/Umbrella

Keywords

Federated Identity Management, Supporting Research Communities

Abstract

Over the past years, many NRENs have successfully built national federations by deploying authentication and authorization infrastructures (AAI). GÉANT designed, developed and launched eduGAIN [1] to support cross border use cases and as more and more federations become members of eduGAIN, the foundation for delivering federated identity is solid.

Meanwhile, fine-grained access management of research data has become a topical issue in science. e-Research projects and infrastructures, driven by the interest in using Federated Identity Management technologies in 2012 produced a paper called 'Federated Identity Management (FIM) for Research Collaborations'[2]. This paper provided requirements for the usage of federated access from various e-Research communities and identified issues towards the wider adoptions of FIM technologies.

Scientific communities stand at different starting points in the implementation and use of the federated identity management technologies by common AAI providers such the eduGAIN interfederation service of GÉANT. Proactivity from the AAI provider perspective to understand the needs of the scientific communities is highly desirable, and *vice versa*; the scientific communities need to learn what to expect to be delivered by the AAI providers.

In GN3plus, the AAI providers of eduGAIN and the scientific communities of FIM4R (Federated Identity Management for Research) have teamed up to deliver a series of pilots that address some of their challenges.

The pilots are:

- ELIXIR [3] – integration of European Genome-phenome Archive and Resource Entitlement Management System

- DARIAH [4] – integration of DARIAH-DE services for digital humanities
- Umbrella [5] – bridging between the Federated Identity Solution of the Photon and Neutron Community and eduGAIN, including support for non-web Single Sign-on.

Common work between all the pilots has been the identification of three different architectural options for using eduGAIN:

- Option A: Add services via an existing federation
- Option B: Create an own federation
- Option C: Join via a Hub or Proxy

Together with the individual pilots, GÉANT helps identify and support implementation of the appropriate architectural option for using each community. In addition, each community pilot has a different range of challenges to be addressed specific to their needs.

ELIXIR

Accessing and computing with large data-volumes from modern biology comes with a specific set of challenges on technical infrastructure and the ELIXIR Technical Services Programme of Work delivers solutions of wide-spread utility in the life-science domain. The services related to AAI must be sustainable so that specialised bioinformatics service providers can rely and build on them [6]. ELIXIR will clearly have to collaborate closely with the European e-Infrastructures to address user needs and fully integrate into the European technology landscape.

The current ELIXIR activities on federated authentication enable governance processes and access to personal genome data through institutional logins and automated interaction with appropriate data access committees. ELIXIR technical service requires federated AAI for user authentication and authorisation procedures by ELIXIR services at varying assurance levels that fit the biomedical data requirements. For sensitive data technology identity federations must offer a means to assess how well users having access to data are identified [6, 7].

One major conclusion from recent the ELIXIR technical coordinator workshop in May 2013 was that while cloud technologies and virtual machines offer great potential to host a variety of computing needs close to the data, there is an urgent need to provide and continuously develop software services to meet the biological end-user data analysis needs and that deploying virtual machines on top of the cloud service offerings is a good approach. ELIXIR Technical Services will collaborate with translational and biobanking infrastructures at both the European and national level to ascertain that there are effective services to securely access and exchange data. Federated Identity is a key enabler for this.

DARIAH

The aim of the DARIAH pilot is to integrate the DARIAH-AAI with with eduGAIN. DARIAH-AAI was established within the ESFRI Digital Research Infrastructure for the Arts and Humanities and consists of web-based services that are protected by SAML Service Provider (SP) and a LDAP based user management system allowing for role based delegation of administration rights within a European hierarchy of countries. DARIAH also operates a Shibboleth[8] Identity Provider that acts as authentication authority for homeless accounts and as an attribute authority for all DARIAH users. All services make authorization decisions based on memberships in privilege groups that are managed in the LDAP server. Via the attribute queries of shibboleth service provider this membership information is transported to the services.

The pilot work plan includes the technical description of the DARIAH AAI and the technical aspects of eduGAIN integration, for instance concerning the attribute query based authorization. Other work items include profiling DARIAH users, establishing trust via the GÉANT Data Protection Code of Conduct and contacting and negotiating with impacted federations and home organisations. Since DARIAH aims to federate with other ESFRI activities in the fields of humanities and social sciences it represents a broader community in this pilot. This community is considering future plans for AAI, including the possibility of a federation for social sciences and humanities connected to eduGAIN.

Umbrella

Umbrella is the pan-European federated identity system for the users of the European large photon / neutron facilities. It provides an EU-wide, unique, persistent user ID and enables users manage their own entries, supervised by user offices. Users of photon/neutron facilities are highly mobile and cross-discipline. Up to 40% of users perform their work at multiple sites, from fields such as Matter and Material, Energy and the Environment and Human Health. This inspired the creation of Umbrella as a system commonly developed under a number of EU projects.

Umbrella supports optimisation of process from experimental data acquisition to data publication in this environment. By bridging between Umbrella and eduGAIN, Umbrella users get increased flexibility without introducing another account. Challenges in credential translation and user friendliness are addressed in this pilot. Trials of Moonshot [9] technology will also allow remote, federated access direct to experimentation facilities for the first time.

Acknowledgements

The authors wish to thank the FIM4R community, chaired by Bob Jones (CERN), the GN3plus SA5 Enabling Users team, lead by Lukas Hämmerle, the REFEDs community, ELIXIR AAI pilot manager Mikael Linden. European Genome-Phenome Archive technical lead Ilkka Lappalainen EMBL-EBI.

References

[1] FIM Paper https://cdsweb.cern.ch/record/1442597
[2] eduGAIN http://www.edugain.org
[3] ELIXIR http://www.elixir-europe.org/
[4]DARIAH http://www.dariah.eu/
[5]Umbrella https://umbrella.psi.ch/euu/
[6] ELIXIR AAI pilot report https://tnc2013.terena.org/core/presentation/18
[7] 6th FIM4R report https://refeds.org/meetings/oct13/index.html
[8] Shibboleth Federated Identity Solution http://shibboleth.net/
[9] Moonshot https://community.ja.net/groups/moonshot

Vitae

Ann Harding

Ann has worked for SWITCH since 2007 and is currently in the AAI team. She leads the GN3plus Activity SA5, Application Services and works with a particular focus on supporting research communities. Before joining SWITCH, Ann worked for HEAnet from 2000 to 2007, as a network engineer and, from 2002, as Network Operations Manager. She was also co- chair of the TERENA Task Force on Lifecycle and Portfolio Management for NRENs. Ann has gained third-level qualifications in Arts and Humanities and Computer Science and a Master's qualification in Cultural and Media studies.

Peter Gietz

Peter is founder and CEO of DAASI International GmbH, a spin-off from the University of Tübuingen. With his company, since 2001 he works in the fields of identity management, federations and research eInfrastructures. Since 1994 he worked for the DFN projects on X.500 and LDAP, which he lead in the last phases. From 1998 to 1999 he worked for DANTE, Cambridge, where he was responsible for the NameFLOW project and maintained the root of the international X.500 Directory. Between 2008 and 2010 Peter was also employed by the University of Heidelberg, where he chaired the IT department of the Cluster of Excellence „Asia and Europe" and with his team designed and set up the cluster's virtual research environment "Heidelberg Research Architecture". Peter was involved in a number of research projects in the fields of PKI, grid computing and eHumanities, such as TextGrid and DARIAH-DE. Employed by the University of Göttingen he temporarily lead the DARIAH-DE work package on technical infrastructure for half a year. Peter was Co-Chair of the TERENA Task Force LDAP Service Deployment and has been active in a number of standardisation activities including IETF and GGF. Peter has an MA in indology and science of religions.

Tommi Nyrönen

Tommi Henrik Nyrönen, PhD AdjProf, at CSC – the IT Center for Science Ltd. is the head of the Finnish ELIXIR node and a delegate of the ELIXIR Interim Board. After receiving a Ph.D. in biochemistry (biocomputing), Tommi has worked for 15 years to make ICT services for science both nationally and at the international level. He has published about 50 peer-reviewed papers, been responsible for developing scientific software solutions (e.g. SOMA, REMS), run services and training, and is an inventor in three medicinal patent families. He leads the Finnish partnership in ELIXIR since 2007 in an integrated effort with national biobanking BBMRI and translational medicine EATRIS partner organizations in Finland. Tommi is an adjunct professor in computational drug design in the University of Helsinki, co-founder of FBD Ltd. bioinformatics SME, external member in Biocenter Finland bioinformatics infrastructure network, and a member of the ISB National Graduate School of Structural and Informational Biology board.

Mirjam van Daalen

Dr. Mirjam van Daalen is Science Officer for the SwissFEL Support group and is based at the Paul Scherrer Institute, site of the Swiss X-ray free-electron laser. After receiving a PhD in Structural Geology at the University of Basel, Mirjam worked in industry for a number of years before becoming a Project Manager at ETH Zürich, developing and implementing new curricula for the department of Earth Sciences. Since moving to the Paul Scherrer Institute in 2009, she is responsible for project management for European funding, project management for the European consortium of the SwissFEL free electron laser project and is responsible for scientific outreach for the project.