Title: Federated Identity Management for Scientific Collaborations

Authors:
Daan Broeder, MPI
Bob Jones, CERN
David Kelsey, STFC
Philip Kershaw, STFC
Stefan Lueders, CERN
Andrew Lyall, EBI
Romain Wartel, CERN
Heinz J Weyer, PSI

Keywords: federated identity management, security, authentication, authorization, collaboration, community

Abstract:
Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisation and their network subscribers. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organizations, are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries. As the user communities served by these organizations are growing they are also becoming younger and this younger generation, the Facebook generation, has little tolerance for artificial barriers, many being the relics of technology and policies that could, if reasoned, also evolve. This “Facebook” generation expects to be able to share data, software, results, thoughts and emotions with whom they choose, when they choose. Their boundaries between work and social life are less sharp, and they expect the tools they use to blend into this environment seamlessly. In addition many of the users have accounts at several research organisations and will need to use services provided by yet more organisations involved in scientific collaborations. All these identities and services need to be able work together without the users’ being obliged to remember a growing number of accounts and passwords.

Driven by these needs, representatives from a variety of research communities, including European photon/neutron facilities, social science & humanities, High-energy physics, atmospheric science, bioinformatics and fusion energy, have come together to discuss how to address these issues with the objective to define a common policy and trust framework for Identity Management and secure access to data based on existing structures, federations and technologies.

Many of these research communities are linked to the ESFRI supported Research Infrastructure projects and the discussions have included national and international infrastructures that provide identity related services, standards forums and those

whose responsibility it is to decide what identity mechanisms will be recommended to policy making bodies. While this activity is focused on Europe, the scientific communities have global needs and so interoperation with identity management systems in USA and Asia are essential.

The discussions have been promoted via a series of the three workshops on federated Identity Systems for Scientific Collaborations. The first workshop was held at CERN in June 2011 (https://indico.cern.ch/event/129364) the second at RAL in November 2011 (https://indico.cern.ch/event/157486) and third in Taipei in February 2012 (http://event.twgrid.org/isgc2012/index.html). As a result of these workshops, a common vision for FIM across the scientific collaborations has emerged and the desire to see this implemented with a roadmap and a set of recommendations.

This paper will describe the needs of the research communities, the status of the activities in the FIM domain and highlight specific use cases. The common vision for FIM across these communities will be presented as well the key stages of the roadmap and a set of recommendations intended to ensure its implementation.

Acknowledgements:
UK Natural Environment Research Council

Biography:
Daan Broeder is deputy head of the "Language Archive" a unit of the Max-Planck Institute for Psycholinguistics and is responsible for the group developing the LAT archiving software. He was one of the technical coordinators in the CLARIN EU project and is a member of the CLARIN NL Executive Board.

Bob Jones is head of the CERN openlab project (openlab.cern.ch) which facilitates collaboration between CERN and its industrial partners to study and develop data-intensive solutions for scientists working at the next-generation Large Hadron Collider (LHC). His experience in the distributed computing arena includes mandates as the technical director and then project director of the European Commission co-financed EGEE projects (2004-2010 http://www.eu-egee.org), which established and operated a production grid facility for e-Science spanning 300 sites across 48 countries for more than 12,000 researchers.

David Kelsey is Head of Particle Physics Computing at the STFC Rutherford Appleton Laboratory. He has held security related responsibilities within various Grids (GridPP, WLCG, EGEE and EGI), starting with the creation of the EU Certification Authorities Coordination Group in 2001. This subsequently resulted in the formation of the EUGridPMA and the International Grid Trust Federation (IGTF). Today he continues to lead the development of security policy for both EGI and WLCG and represents these infrastructures inside the IGTF.

Philip Kershaw is a senior developer with CEDA, the Centre for Environmental Data Archival at RAL Space, STFC Rutherford Appleton Laboratory in the UK. He is a specialist in federated identity management and has contributed to the security architecture for a number of distributed systems including the Earth System Grid Federation and Contrail, an EU Framework 7 project to develop a system to support federated cloud infrastructures. He authored and contributed to a number of papers

and abstracts in the area of federated identity management and access control for applications in the environmental sciences domain.

Stefan Lüders, PhD, graduated from the Swiss Federal Institute of Technology in Zurich and joined CERN in 2002. Being initially developer of a common safety system used in all four experiments at the Large Hadron Collider, he gathered expertise in cyber-security issues of control systems. Consequently in 2004, he took over responsibilities in securing CERN's accelerator and infrastructure control systems against cyber-threats. Subsequently, he joined the CERN Computer Security Incident Response Team and is today heading this team as CERN's Computer Security Officer with the mandate to coordinate all aspects of CERN's computer security --- office computing security, computer centre security, GRID computing security and control system security --- whilst maintaining CERN's academic environment and taking into account CERN's operational needs. Dr. Lueders has presented on these topics at many different occasions to international bodies, governments, and companies, and published several articles.

Andrew Lyall, Ph.D., ELIXIR Project Manager (http://www.elixir-europe.org/), European Bioinformatics Institute (http://www.ebi.ac.uk/). ELIXIR aims to create a sustainable infrastructure for biological information in Europe, laying the foundations for the impending biological revolution. Before coming to EMBL-EBI Andrew spent 15 years working in industry, primarily at GlaxoSmithKline, where he rose to the position of Department Head. He has also worked in the biotechnology sector, at Oxford Glycosciences and as a founding director of Confirmant Ltd. Prior to this he worked as an academic researcher at the University of Bristol and the Edinburgh University as well as the Royal College of Surgeons in Ireland. He read biochemistry and computer science at Imperial College and received his PhD in bioinformatics from Edinburgh University.

Romain Wartel is the security officer for the Worldwide LHC Computing Grid. He has been involved in the operational security and policy aspects of several national and international grid projects. He has for example led the operational security coordination team of the EGEE infrastructure between 2006 and 2010. He currently focuses on international security incident response and on improving the collaboration on security issues between different computing infrastructures.

Heinz J Weyer PhD is teaching at Basel University. He was scientific coordinator of the Swiss Light Source SLS and leading author of the Digital User Office DUO in use at most European Photon and Neutron large facilities. As member of the SwissFEL team he is active in several EU projects for the development of the new generation of IT resources for the users at these facilities.