# Summary of the third Federated identity system for scientific collaborations workshop

Bob Jones
IT department, CERN
1st March 2012

This document provides a summary of the workshop entitled “Third Federated identity system for scientific collaborations” that was held at part of the ISGC2012 event on 27 February 2012 hosted by Academia Sinica in Taipei. All the material presented during the workshop is available online: https://indico.cern.ch/event/177418

This was the third in a series of workshops on Federated Identity Systems (FIM) for Scientific Collaborations. The first workshop was held at CERN in June 2011 (https://indico.cern.ch/event/129364) and the second at RAL in November 2011 (https://indico.cern.ch/event/157486). This workshop focused on interacting with the Asia Pacific community and discussing the contents of a draft paper that presents a common vision with a set requirements and recommendations. There were approximately 50 participants from 20 countries across Asia, Europe and the USA.

Dave Kelsey presented an overview of the draft paper and then led a critical review of the common vision and recommendation sections. From the ensuing discussion it was agreed that sections 4 (analysis of common needs), 5 (common vision) and 6 (recommendations) will be revised to present a high-level vision statement, followed by a list of requirements and then a set of recommendations that specify what actions are to be taken by which parties and on which timeline.

Feedback from colleagues in the Asia Pacific region on the draft paper included a summary by Eric Yen which confirmed the relevance of FIM and the status of deployment across Asia. Current activity is primarily for library and scholar services. eduRoam is deployed in 7 countries in the region while the ORCID[1] system is used in 12 countries. Internet2 National Identity Management Federations, based on Shibboleth and SAML, are present in 3 countries while OpenID SSO is used across many countries. Regional Identity Federation activities are conducted by APAN and IGTF. Eric found the analysis in the draft paper useful and that the suggested roadmap will be important. A review of the existing systems will be essential. He highlighted that the majority of the discussions are focussed on authentication which is only one part of the trust framework and most users will want to know if this approach will work in a cloud environment.

Yoshio Tanaka and Eisaku Sakane presented FIM activities in Japan. They explained the work of the Global Earth Observation (GEO) Grid which was set-up in 2006 and uses Grid Security Infrastructure (GSI) and Virtual Organisation Management System (VOMS) for Authentication and Authorization. When migrating to a cloud-based implementation they have found that GSI was not a natural fit so they are exploring the use of OpenID + OAuth2.0 (OpenID Connect). Through this work they are facing issues of Levels of Assurance (LoA)

[1] http://about.orcid.org/

for OpenID providers and the need for common guidelines and profiles for both IdPs and authorization services in a similar style to IGTF.

Another area of investigation is how to federate a set of 9 supercomputing centres within the HPCI (High Performance Computing Infrastructure) project which is currently based on Shibboleth and GSI. While there are technical solutions a number of issues arise at the policy level. They are considering a credential translation between GeoGrid and HPCI.

GakuNin is an Academic Access Management Federation in Japan for academic e-resources. It is based on Shibboleth with about 35 IdPs and 60 SPs in production.

Soonwook Hwang from KISTI in Korea provided input by email before the workshop. KISTI is leading a project called PLSI which is a consortium of 14 HPC computing centres in Korea, intended to link them together to serve as a nationwide distributed computing environment in a similar fashion to PRACE for Europe. With an environment like PLSI, distributed identity management needs to be addressed and Soonwook believes FIM could be a suitable approach.

Valter Nordh presented the eduGAIN interfederation service[2]. eduGAIN is created and being built within the context of the GEANT3 project funded by the European Nation Research and Education Networks (NRENs) and the European Commission (EC). eduGAIN now has 11 federations involved including one outside Europe (Brazil) representing a total of approximately 50 entities. It relies on a full mesh-model where SPs talk directly to IdPs. eduGAIN provides the means for SPs and IdPs to exchange identity related information (attributes) but what gets exchanged is up to the exchangers. IdPs face a security risk when they release attributes to SPs. eduGAIN has published a Privacy Code of Conduct (CoC) (see document attached to Valter's talk on the workshop agenda page) derived from the EU Data protection directive. SPs commit to the Privacy CoC and must produce a Privacy Statement explaining what information they will use and for what purposes. IdPs see SPs have signed the Privacy CoC and this can remove the need for bilateral agreements between IdP and SPs. The CoC currently only addresses the release of non-sensitive personal data within a European context. SPs are self-auditing in the sense that there is no external body which verifies if their Privacy Statement is consistent with the eduGAIN CoC. eduGAIN is soliciting feedback on the CoC and template Privacy Statement with a public review process scheduled for April 2012. Comments should be sent to Mikael Linden at CSC.

Roberto Barbera described how they have widened the number of e-Infrastructure users using Science Gateways and Identity Federations. He highlighted the use of FIM to simplify the adoption distributed computing systems. Roberto mentioned the IDEM (www.idem.garr.it) federation in Italy, managed by GARR (the Italian NREN), that has 38 IdPs and 35 SPs and serves the Italian higher education and research community. The number of IDEM members is estimated at 3 million that corresponds to about 50% of the whole number of students/researchers in Italy. The IDEM federation is part of eduGAIN. Technical solutions have been put in place to link the IDEM federation to the science gateways for a number of research communities (including humanities and life sciences) and the grid based distributed computing infrastructure where pre-defined applications are executed.

[2] www.edugain.org

Heinz J Weyer gave an update on the Umbrella project investigating FIM for the European Photon and Neutron facilities. Umbrella is being pursued within the context of the PaNdata[3] and CRISP[4] projects. The design foresees the creation of a new, centralised IdP serving the European Photon and Neutron facilities which represent SPs in their FIM model. The project has progressed to a testing phased with 30 users across Europe and 4 facilities (DESY, Diamond, ESRF and PSI). An extension to Umbrella is being planned to allow a two phase review of proposals (i.e. via two separate committees) that will handle controlled access to proposal data.

In terms of next steps, the following points were agreed:

The draft paper will be revised as descried above taking into account feedback and discussions from the workshop. Key stages of the roadmap will be added. Additional feedback can be provided on the draft until 8th March 2012.

Each community should then discuss the paper and it recommendations. During this step we can make sure it represents the “end user” point of view and not only that of facility operators.

The paper has been accepted for presentation at the TERENA Networking Conference (TNC2012) in May 2012. This will be an opportunity to get feedback from TERENA and the NRENs.

At the forth workshop, scheduled for June 21-22 at MPI Nijmegen in the Netherlands, the user communities will be asked to confirm their endorsement of the paper. It will also be the occasion to provide updates on the pilot projects (i.e. those similar to Umbrella) from the other user communities. The roadmap steps should be expanded and the best means to engage technology and service providers (commercial and public) as well as funding agencies should also be discussed.

[3] http://pan-data.eu/

[4] http://www.crisp-fp7.eu/