Summary of the 5th FIM$_4$R Workshop

This document provides a brief summary and the minutes of the workshop "5th Federated Identity Management for Scientific Collaborations", held in Paul Scherrer Institut on 20-21 March 2013.

All the material presented at the workshop is available online: http://indico.psi.ch//event/2230

In the past workshops, the FIM subject was addressed to be a concern for any kind of community. Requirements for different communities vary from each other. But, specifically in the research communities there is an interest in a common approach to FIM, as it would benefit to join efforts. Therefore, the participating research communities agreed on a common vision for FIM, enumerated the different use cases and addressed some common advisory guidelines. This all is gathered in a paper presented at the TNC in April 2012: https://tnc2012.terena.org/core/presentation/23. This paper has been reference for different projects aiming to a common solution, like TERENA, NRENs and the new GEANT3+. Indeed, this document is considered to be mature enough and will not be updated further other than including the prioritisation of the already documented requirements (see appendix).

Fruitful discussions were possible thanks to the approximately 45 participants, coming from Europe, Switzerland, USA. Besides, some new communities have participated, for example ESA and WeNMR.

The workshop is divided into 3 sections:

- A major topic was to present and discuss several FIM prototypes currently in development.
- Second, as the term 'federated' already indicates, it will not be possible to find a 'one size fits all'-solution to all requirements. In addition, there are, especially in the commercial sector, already various existing identity management tools, which would be interesting to connect. Bridging and inter-federation developments have been allocated into this section.
- Another section of this workshop was to comment on FIM4R paper and to technical discussions.

Bob Jones opened the event by mentioning the goals to be achieved:

- Geant3+ presentation and possible engagement with presented solutions.
- Evaluation of prototypes in terms of technology interoperability, status, plans.
- FIM paper/discussions.

Next sections examine each of these mentioned points.

Geant3 +

The new Geant3 + (G3+) is an EC co-funded project starting in April 2013. This project has been proposed by TERENA and GEANT, and presented by Ann Harding in this workshop. Its goal is to implement a common framework on AAI. It brings the opportunity for developing/implementing the best positioned existing solutions. Positive evaluation of a prototype, therefore, might lead to engagement with the G3+ project, which has an expected duration of 2 years. Hence, it tries to enhance those solutions that have a short timing plan, within approximately one year, to be implemented.

Pilots and Projects

Next is a very brief table with the solutions presented during the workshop.

	Technology	Inter-federation	Status	Plans
ELIXIR	SAML2	Joined to the HAKA federation.	Development	Join eduGAIN and Kalmar union.
ESA	Shibboleth		Production	Join NASA and EUMETSAT
WLCG	Web based and non-web based. Pilot project on non-web based. SAML2.		CLI solution achieved, but looking into alternatives.	Refocus on web-based use case.

DARIAH	Shibboleth		Production (with own IdP)Interconnect DARIA-EU, first attempt with interim solution, ultimately via eduGAIN	
SWITCH	Shibboleth	Open to inter-federation with eduGAIN.	Production (for the majority of Swiss Universities)	Moonshot and Interfederation with eduGAIN
CLARIN	Shibboleth		Implementation	Interconnection through Service Provider Federation (SPF)
Umbrella	Shibboleth	Bridging concept being developed.	Implementation	Affiliation Database, Sync with other programs iCAT, Moonshot. Bridging. Implementation up to Sept. 2013.
WeNMR	Drupal based WeNMR VRC, Shibboleth authN, phpCAS authN, robot certificates.	Flexibility to connect to a wide set of federations (from Drupal).	Production	
SyBIT	Azure	Any federation could be easily integrated.	Microsoft product.	Self-federation model.

Below some notes, remarks and questions from the talks are summarized:

ELIXIR AAI PILOT – life sciences

ELIXIR EGA AAI project is part of the work of the project led by European Bioinformatics Institute (EBI) where CSC, who is also the Finnish NREN, is actively developing AAI solutions. EBI has specific requirements regarding restricted access to data sets relating to genomes, where permission has not been granted by the individuals involved in the study. This is the focus of the European Genome-phenome Archive (EGA). There are 323 datasets, with about 370TB, 200,000 samples. This quantity tends to double every 8 months. EBI (http://www.ebi.ac.uk/ega) is a secure broker for making this information available effectively.

The pilot is divided into 2 pilots:

Pilot 1: Federated authentication. It consists of integrating the EGA web portal with a SAML2 SP. This phase is very sensitive and it cannot be given to a third party. A scenario was described where usernames are actively shared within each research group and that these credentials continue to be used by researchers who have left the project, and whose access should have been revoked. There is a strong need to control this kind of situation.

EBI has joined the Haka federation, and the intention is to interfederate using eduGain and Kalmar.

Pilot 2: Authorisation management. This process is complex involving aData Access Committee (DAC) that ensures ethical conditions are respected when providing access to the data-sets.

A five minutes demo video of the current system was shown. It demonstrates federated authentication, authorization and revocation of authorization.

This pilot plans to be in production for ELIXIR soon and also to make it available with an open source license.

Questions:

- Negotiations with EMBL were complex, because they are unware of the implications of Federated Identity Management. The main concerns were related to liability and jurisdiction aspects for the SP.

- Protection of the real data comes also from the impossibility of downloading it. It would be allowed to visualize it.

- To the question of accomplishment of a risk assessment, the answer was that this is foreseen to be done at a later stage of the pilot.

- Delegation of Authorization supported? The REMS systems supports an approach that each data access application has one “Applicant” (the person who fills in the application on behalf of the research group) and potentially several “Members of the application” (persons to whom equal access rights are applied as well). The leader of the research group (aka Principal Investigator) can list a hypothetical grad student in the data access application, and if the application is approved, this grad student can access the data using his/her home university’s username/password, by virtue of the federated authentication.

- How is the privacy of the researcher protected? The researcher’s data access applications are visible only for the person or body (such as an ethical committee) that processes the data access application (and to the applicant him/herself). The ethical committee cannot see the data access applications that are sent to other ethical committees.

ESA EARTH OBSERVATION SSO- Andrea Baldi

At ESA they have been deploying a Federated Identity Management system since 2011. A general FAQ is found here: https://eo-sso-idp.eo.esa.int/idp/umsso20/login?faq. This is the entry point to the SPs: https://eo-sso-idp.eo.esa.int/idp/AuthnEngine. And these are the initial set of SPs accessible: https://eo-sso-idp.eo.esa.int/idp/umsso20/login?esasps

A Shibboleth infrastructure was deployed. The design includes a redundant IdP (i.e. 2 instances) and an LDAP hierarchy for the Service Providers. This hierarchy consists on few master SPs that can be inherited by others. There are 2 administration roles: one for user to manage their own profile (for example to recover their password via secret question/answer), and another for a more advanced way of administering. Since the complete infrastructure is controlled internally, there are no issues of releasing attributes.

This infrastructure is in operation having more than 10,000 users. Data Protection and privacy shall follow soon EC regulations.

Besides deployment, also development activities have been accomplished. A java client library has been developed (based on Apache HTTPclient) to offer an SSO API to java applications.

Medium objectives are to connect to other space partner’s federations, having in mind NASA and EUMETSAT.

Questions:

- Is security officer aware of global standards? Followed ESA CERT consulting body.

- They don’t support command line applications.

- Pushing of attributes from SP to IdP is made as an extension by ESA themselves.

- Looking into the creation of dynamic accounts and into ECP extension for SAML2.

Identity Federation in WLCG/HEP – Romain

A pilot project is being developed in the WLCG. It is based in the non-web based case. The goal is to make transparent the management of the x509 certificate process. More information about this Pilot project is available here https://twiki.cern.ch/twiki/bin/view/LCG/WLCGFedIdPilot. The key idea is to issue x509 certificates with home-issued federated credentials. A tool for solving this already exists in the US: the CILogon, which is used for enabling the generation of x509 certificates. The authentication is done through the IdP and the authorization is left to the Virtual Organizations. CILogon together with the EMI STS (http://www.eu-emi.eu/security-token), which manages translation of credentials, are used in the pilot project.

The ECP component is needed in order to use the CLI pilot project, but feasibility it is yet to be evaluated, as this implies that all the IdP’s must adopt it. This is expected to be very difficult to achieve, especially since not all the users need it, therefore other solutions, without ECP, are being explored. This investigation is supported by CERN and will require more time and effort than expected and so at the moment the pilot has been paused.

Other issues are addressed: definition of Trust and Level of Assurance, requirement of attributes, and a deployment model for WLCG.

Questions:

- There are many sources of recommendations, it is helpful to check the IGTF guidelines for identity vetting.

- It was pointed-out that Authorization relies on sites, therefore it is assumed that sites check their users, which might become an issue.

- How to remain synchronised outside the FIM4R meetings? This question was retained for the discussion section.

- Is Moonshot on the agenda? Indeed it was considered in the very early stages of the pilot project, but the requirements to deploy in each site are too high. The issue of getting IdPs to deploy a different mechanism is a blocking factor. Besides, it has been studied that Moonshot does not really satisfy all the requirements. In this respect, it has been asked that the evaluation criteria needs to be shared.

FIM4DARIAH- Peter Gietz

DARIAH is in the context of humanities research community activities.

DARIAH EU federation is in the process of being built on basis of SAML. A group based privilege management for VOs implemented by DARIAH-DE is already being used within the larger European DARIAH context. DARIAH is being established as a European Research Infrastructure Consortium (ERIC). This legal framework will facilitate the long-term sustainability of DARIAH. DARIAH-EU is divided into four Virtual Competency Centers (VCC): e-infrastructure, research & education, scholarly content management and advocacy.

The work in production is based on an own Identity Provider for homeless (i.e. without academic affiliation, or affiliated with institutes not participating in federations) users and hoping for eduGAIN to provide a European interfederation. The problem they find that is delaying eduGAIN deployment is that not every national federation participates or not every IdP delivers the necessary attributes to eduGAIN, not even the eduPersonPrincipleName. As a solution to this problem, it has been proposed to use targeted ids, and map them to identities in DARIAH IdP. DARIAH uses LDAP, openldap, for authentication and authorization, and on the federated side Shibboleth is used. Temporary federation solutions could be to unite with CLARIN SP federation or co-setup a federation in the frame of DASISH project.

In the federation there are Resource SPs and a Registration SP, that collects data from the user, that were not provided by the campus IdP. With the group based privilege management components, national representatives will be able to create organisations and delegate group management privileges in the LDAP server to administrators in a hierarchical way.

OAuth2 and OpenID Connect are being integrated into the DARIAH SAML2 based infrastructure.

Questions:

- In order to create the federation, and since eduGAIN is not currently a solution, a “temporary” solution is to have their own IdP.

- When using SAML ECP for non browser based applications (e.g. web services) every delegation has to be configured in Shibboleth IdP which is not a scalable solution.

- How many users and what administration load? 400 users in LDAP, and increasing. Therefore distributed management is foreseen.

- Some web based applications still have for now direct authentication against LDAP.

GEANT Data Protection Code of Conduct- Mikael Linden

This is the Code of Conduct document: https://refeds.terena.org/images/f/fc/GEANT_DP_CoC.pdf

An IdP takes a risk when it releases attributes to a SP. IdP may become liable if the SP is hacked and the personal data is spilled onto the internet. Hence, IdPs hesitate to release attributes. This document aims to ease the release of attributes by reducing IdPs hesitation.

There has been a pilot project from the CLARIN community, involving 3 federations: Finland, Germany and Sweden, altogether 4 IdP and 7 SPs. This pilot has been documented and has been publicly shown online for comments. Results are available here: https://refeds.terena.org/index.php/CocPilotReport

The plan is to have the CoC in production by Q2/2013. Also to submit an article to the 29th Working Party Q2/2013: the EU body contributing to the uniform application of the Data protection directive.

This pilot project shows that more documentation required for SPs (e.g. templates, & training) including “How to write a Privacy Policy document” and guides on what attributes are necessary for a service.

Comments:

- CoC is fundamental. Internet2 is also proposing the CoC to be considered by the US Government.

Advancing Federated Technologies for different communities – Licia Florio

The AAA Study document has been delivered, in draft version, and it is still open to comments. The main goal of this document is to evaluate the feasibility to harmonize AAIs, and also to deliver a prototype infrastructure, as well as enhancing existing ones. The approach followed was to understand the AAA requirements, study the existing AAIs and identify their gaps. This document includes policy and practices recommendations, i.e. Harmonization. There is not an AAIs that satisfies all use cases, but the majority of the communities are willing to participate to federate access.

Further, Licia asked for a list of the use-cases for FIM4R.

The EC proposes a roadmap for collaboration.

The presentation had a second part: “Addressing e-research Requirements”. In this part, several proposals were listed:

- To develop a roadmap as a joint activity between ID federations (REFEDS/GEANT) and research communities.

- Discussion group to be created: who should do it and who wants to participate?

Questions/Comments:

- Research data alliance hasn't got working groups on Federated Identity Management yet. Left for the discussion section.

GEANT3+ - Ann Harding

The goal is to implement a common framework on AAI and to enhance those solutions that have a short timing plan, within approximately one year, to be ready to deploy.

There are 4 subjects to work:

- Non-web based applications

Looking at OAuth, SAML ECP and possibly OpenID Connect, Abfab (Moonshot) but Moonshot and ECP will not be in production by next year (still in pilot phase). We should identify how urgent the problem is. In this respect, it was anounced the pilot project that Moonshot is starting in April.

- Guest IdPs

Who will operate Guest IdPs? Google and Facebook as Guest IdPs? It has been proposed to have a working group to refine requirements in this subject.

- Attribute Authorities

Do we have any good examples that exist today (e.g. ELIXIR EGA AAI pilot, maybe DARIAH)? The proposal here was to identify possible models to use external attribute providers, select some models and test them.

- Motivating IdPs to release attributes: It is very important that IdPs release attributes.

There are a couple of concepts important to work on: Federation as a Service as well as Interfederation.

G3+ is looking for 2 or 3 use-cases linked to the pilots that can produce results within the lifetime of G3+ (2 years starting April 2013) where these results could be applied to other communities.

To start up with this innitiative, Ann asked for a list of use-cases by the start of May 2013 . This topic will be in the discussion section.

Questions

- Federation as a Service is a goal to be achieved? Do not know yet.

- How is the idea of interfederation? There are about 18 Federations in Europe, and even more NRENs. Also in the US will be many federations (by states, market sectors etc.), therefore interfederation is naturally needed. Is there an idea of community federations to bigger/super federations? The answer points to eduGAIN as an appealing possibility.

Managing identity- ORCID and Federated Login- Laure Haak

Laure Haak, Executive Director

ORCID a non-profit organization that provides an international registry of persistent and unique Identifiers for researchers and scholars. The mission: connecting research with researchers. The ID obtained consists of a 16 digit number expressed as an URI. Registration, use, and search of the Registry is free, and requires only name and email address. ORCID does not collect date of birth or passport information. There is no vetting process during registration; validation is accomplished by embedding the iD in sysmte workflows such as university personnel systems and manuscript submission. he user can configure the visibility of their information, there are 3 levels of privacy, from public to completely hidden, but the userID is always public. ORCID has users from over 200 countries, and has (as of the time of the meeting) more than 85000 registered users.

This is the link to get registered: http://orcid.org/register. Registration takes less than a minute. The ORCID iD is being integrated with several workflows: university personnel systems, manuscript submission, grant applications, linkage with repositories, linkage with other IDs. Several publishers including Nature, Hindawi, APS, Copernicus, are already requesting ORCID iDs during manuscript submission, and others are in the processor embedding including Springer, Wiley,Elsevier, and a number of association publishers such as MLA, APA, and ACSESS. ORCID is also working with vendors and offers service provider membership options.

Individual iDs are completely free of charge, the business model comes with organisations, for example, CERN and EMBL are member organizations, and they are charged a fee for using the member API.

The advantage of having an ORCID iD is that it offers a registry for resilience, and the iD is 'owned' by the researcher, is completely portable, and is (through workflow integration) becoming part of the metadata associated with a researcher's works (papers, datasets, etc). Embedding in local systems can provide a route to support FIM, and also can assist with reporting on research outputs.

Questions/comments:

- It is a completely distributed organisation.

- Can be used to fix Scopus entry.

Towards FIM as a Service: FIM for the Contrail Cloud Project – Philip Kershaw

This is the link of the project: http://contrail-project.eu

They are building a system for federating multiple cloud providers, including open-source and commercial.

OpenNebula is used as a basis, and plugins are being developed to support FIM, specifically to OpenID and Shibboleth.

One of the difficulties presented is that cloud service providers have limited understanding of FIM.

The 'delegation problem' was at first a bit difficult to be solved, since automated services call on other services on behalf of a user, and this becomes a problem when the services are shared with other projects (such as CLARIN). Delegation is essential (chose identity credentials not authorisation – so like proxies) and it has been solved using OAuth 2.0

CEMS OGC are using the OAuth modules and so are CLARIN and EUDAT.

Finally a short demo video was presented showing how the module developed could be re-used.

CRISP (PSI/GSI) Umbrella Bridging – Bjoern Abt & Almudena Montiel

It will not be possible to find a ‘one size fits all’-solution to all requirements, therefore the need of a bridging initiative has been detected in the context of Umbrella. Bridging means to join different Federations. In order to follow the philosophy of Umbrella, the bridge is built always as a user initiated action. Also, there is no cross federation exchange of attributes.

The bridge is implemented in a persistent way by keeping 2 new objects in the Umbrella system: an AccountLinking table, where the link to the different accounts is stored, and an AttributeMapping table, where mapping of attributes between the different federations and Umbrella are kept. The Umbrella ID is considered a meta-account through which a user can access to any of the services offered by the federations bridged.

A proof of concept has been shown with a live demo, connecting the x509 use case from FAIR-GSI to one of the Service Providers in Umbrella.

SWITCH – Lukas Hämmerle

Switch is involved in AAI with the SwitchAAI federation (and edugain) that provides access to web services, and eduroam to provide network access. The past of AAI is preceded by the VCS (Virtual Campus Switzerland), a federal program (200-2008) to promote e-learning. SWITCH has led the process of FIM in the Swiss universities.

The services provided by SWITCHaai include: different kinds of documentation, call-in helpdesk, discovery service, attribute viewer, resource register, virtual home organization, guest login, group management tool, toolbox (solution for VOs). SWITCH also developed some code: uApprove, x509 login handler, kerberos login handler.

The current status is shown: 98% coverage in higher education AAI – enabled accounts, 100% Shibboleth for Home Organizations, and the resources provided are 96% Shibboleth.

One speciality is the Attribute Release, which is not very much of an issue in SWITCHaai, it is completely automated via Resource Registry web interface by the IdP admin. Default rules are applied to SPs. Admins get automatically informed of the changes.

Success factors: Virtual Campus Switzerland funding, big acceptance due to involvement of the universities and large Universities participating increase the critical mass.

Eduroam compared to AAI has a smaller coverage. It happens that many universities mutually allow access to their VPN servers from the Wifi network (therefore users can open VPN connections to their home institution in a foreign Wifi network) or that they offer open Wifi.

The future topics: monitoring with AMAAIS. Also, it is intended to get a bigger coverage in Higher Education by extending to upper secondary organisations. There is a need for inter-federation, the proposal is eduGAIN. For the non-web based case the proposal is to use Moonshot. Moonshot = eduroam + AAI (eduroam spread all over Europe + large part of America)

Questions:

- What does it mean in terms of funding to provide a service in the inter-federation. There is a stable model for funding, and much effort comes from the local Universities. SWITCH is rather coordinating, the heavy work is done in the local Universities.

- How is it possible to Release Attributes automatically: attribute specification makes it possible to automatically distribute them, because it is homogeneous.

FIM FOR THE SSH – Daan Broeder & Dieter Van Uytvanck

SSH= social sciences and humanities disciplines.

ESFRI CLUSTER project for the SSH. CESSDA (social), CLARIN (language), DARIAH (humanities), ESS and SHARE. DASISH uses previous CLARIN work with FIM as a basis.

CLARIN and DARIAH accept FIM, but CESSDA is more problematic because there is a tradition to centrally manage users, they are very concerned about the sensitive data and especially about the different security levels.

On-going project: CLARIN Service Provider Federation (SPF): is an organization of SPs that provide services to EU wide base of users of language data and technology, eduGAIN is an alternative to this. The goal of SPF: connect 11 SPs to 3 national IdFs, to demonstrate the feasibility (both technically and legally) to create a border-crossing federation infrastructure. More info at: http://www.clarin.eu/spf. CLARIN ERIC could become the legal entity as contracting party.

Dieter Van Uytvanck talked about facts/status of the SPF: about the Release of Attributes issue, the only problematic parts were some German universities which refuse to release personal data. According to Dutch IdPs releasing attributes there are some issues to release them due to opt-in. eduGAIN and the Code of Conduct could help in this issue. The opt-in issue does not scale, simply mailing IdP admins did not help and so now they target high-profile CLARIN affiliated people (department heads, directors etc.) which gives better results.

Future steps: work towards a SSH federation with DARIAH, either extended CLARIN SPF or something else: eduGAIN. Include those CESSDA centers that can join and investigate hybrid topologies integrating islands with central user management.

Questions/Comments:

In the US there are 3 security levels, it would be interesting to compare such levels of security.

eduGAIN – metadata without policies alignments experiments. In the audience it was suggested to have a look at the PEER experiment (https://spaces.internet2.edu/display/PEER/PEER+Project+Plan+and+Proposal)

Umbrella- Mirjam van Daalen & Bjoern Abt

Many European projects are involved in Umbrella, therefore a big community of users.

Concept of Umbrella: Umbrella on top of Web User Offices (WUOs), and providing a unique persistent European-wide identifier. This Umbrella-ID would be a meta-account that could be linked to any other account from the WUOs, and through this link, successful access can be accomplished. In this way, only the authentication phase is present in Umbrella, the authorization is left to the local WUOs.

Defined the WP3 inside PanData and the WP16 inside CRISP, there are different parts of the project for each of the work packages. Umbrella is the basis for various user services under development. There is a natural need of coordination in between all the partners, and in order to harmonize the activities there are bi-annual Harmonization meetings organized by PSI.

Without a unique identifier it will not be possible to have unified access and work with common tools.

Bjoern Abt explains the technical part of the tool. The project is currently in implementation phase. At the moment a master-master replication for LDAP servers in each lab is being deployed. Another part of the design consists of deploying GEO DNS to ensure users get connected to local IdP. First facilities for implementation will be ILL, ESRF and PSI. Open to all users by September 2013.

Questions:

- Why 4 IdPs? Mainly for political reasons: everybody is interested in having their own user data set locally, and technically it makes load balancing possible. Confidentiality of data and activities of users is essential for the labs.

- What exactly does *Data Protection* mean in Umbrella? It means the protection of the proposals, and the data during the whole process. Different synchrotron and neutron facilities must not see proposals of other facilities because of high competition. A 3 years embargo period for data is normal in this community. This data belongs to the user and nobody else can access it. Technically feasible, but the policy is a different issue.

In conflict with OpenAccess. Privacy is ok, though.

- Community: More than 30,000 users. 40% of users perform experiments at multiple labs. A survey is done every year about the functionality and more aspects of Umbrella.

Centralized user management and SSO for the WeNMR gateway through the WeNMR – Marc Van Dijk

WeNMR aims at bringing together complementary research teams in the structural biology and life science area into a virtual research community

Demo of the portal (written in php): http://wenmr.eu/

The motivation was to join all the portals of the community through a single IdP.

In the demo a login SSO with a grid certificate is shown. Also, access to WeNMR Grid-enabled portal is shown.

Questions:

- The protocol to send SSO credentials with the portal is a non-standard protocol. The protocol was developed by themselves, which is actually close to the protocol used to connect to banks from mobile phones (encrypted string of time stamp). The reason: simplicity.

- Was any problem found in managing metadata so far? No.

- Authorization is completely separated from Authentication, but both processes are managed from within the portal. The AuthN is implemented in a core module of Drupal.

- User interface for dealing with several ways of authenticating: it was done with Drupal.

- Connecting to other federations is technically possible.

- At the moment it is in testing phase.

Web SSO with Cloud resources using ADFS - Dean Flanders

SystemsX: http//systemsx.ch, world-leading initiative in quantitative Systems for Biomedical Research, lies in the border between Industry and Research. It is located in Basel, Switzerland.

First it was mentioned that the lack of FIM is impairing research. Mentioned the example of “onelogin” as a company offering enterprise identity management http://www.onelogin.com/

The key technology would be Microsoft ADFS. It is possible to make a generic integration of any kind of federation though ADFS.

A proof of concept has been done integrating with Umbrella federation from PSI.

The concept of self-federation is essential:

- Self-federation Portal: self-federation Tool follows a hybrid model. Self-federation concept is vital to an all inclusive federation necessary for research and potentially avoids many discussions.

Technically all components are available for making FIM a commodity item.

A trusted platform like Azure offers a valuable low cost federation backbone.

Federation should be under the control of the institution and attribute management under the management of the user.

Next step is to make a fully functional version with Azure AD with multiple organizations.

Questions:

- Multiple institutions under same federation, how to keep all under control?

Idea: institute provide resource x, y, and c to federation and the users have to be responsible.

- Why being against Facebook? Because it does not offer any link from the user to known affiliations.

The DHCP-RP project: requirements and implementations of federated access to digital cultural heritage contents – Maria Laura Mantovani

Digital Cultural Heritage- Roadmap for Preservation.

13 participants in DHCP-RP: ICCU (coordinator), Italy.

The goal of the project is to prepare a roadmap for preservation, cover digital cultural heritage aspects, conduct a coordination action within EUFP7, federated e-Infrastructure.

Survey about Identity Management had these results:

- Use cases:

Web portal (Internet Culturale).

Magazzini Digitali: deposit of Italian publications.

- What kind of data want to be shared?

Text for metadata, web copies of digital objects.

- Why user needs authenticating?

Need to identify people, coming from different institutions.

- Which kind of authorization is wanted?

Authorization mapped to roles in a workflow schema, respecting the policies.

e-CultureScienceGateway as a tool for Cultural heritage community is a web portal that interfaces users to e-infrastructures like grids.

Federated authentications: support of national identity federations and could join other federations.

More info: http://www.dch-rp.eu/

Question:

- Why are you in favour of facebook (social networks)? Because there are "homeless" users that belong to no national institution, and it was an easy way to link them to the system.

FIM paper

Some remarks about the paper were presented for the audience not present in the previous FIM4R meetings. In this paper requirements were prioritized[1] and recommendations were listed. Besides, this paper has served as a basis for the joint work between Terena, NRENs and it will be a refence also for GEANT3+. FIM is recognised by several ESFRI projects: BioMedBridges, CRISP, DASISH, ENVRI.

This paper has reached a mature status and it is preferrable not to update it anymore. If there is a need of updating or adding info, some other documents should be started.

Discussion

- FIM4R paper:
    - added prioritization of requirements.
  - Propose that we don't touch the document any further and concentrate in other material.
- Technical discussions:
  - How to carry that in between meetings: Put together a list of lists where specific subjects can be discussed. For ex. Re-use the REFEDS emailing list for eduGAIN related points.
    - Proposal for using a TERENA REFEDS wiki to communicate.
    - Ken suggested to have a list of recommendations added from Internet2.
    - Ken proposed that the technology and service suppliers produce webinars to explain some the technical advances regarding identity management.
  - All people registered in the workshop will be added to the federated-identity mailinglist. Everybody agreed.
- Working with Geant3+
  - Community representatives should document use cases (max 1 page each) by **19th April**.
  - Community representatives to propose which of their use-cases they like to pursue with Geant3+ **26th April.** Dean Flanders thinks a use-case oriented approach is not going to be useful for its case, but Geant3+ answers that they are actually more flexible than that. Bob Jones clarifies that communication is not limited to that, therefore other ways of describing are of course welcomed.
- Research Data Alliance (RDA) http://rd-alliance.org/: Daan Broeder presents RDA. It consists on bottom-up solutions rather than top-down. He mentioned the example of IETF, where they make an effort for interoperability and they are successful in terms of standardization, producing numerous RFCs. There will be working groups, the workflow is as follows: a case statement is announced, this needs to be approved (not sure about whom), and then work may start. There are 2 chairs: European and American. The description of the work and work-plan is in form of deliverables that must be finished within 18

[1] See Error: Reference source not found

months. They focus on real implementation. Supported by America, Australia and Europe. Data foundation and technology.

- Should there be a working group about FIM? They already tried in the 1st plenary meeting, with no much success. They will try again in September (2nd plenary meeting). If not with FIM specifically, with something more generic (AAI).
- Heinz Weyer asks about the European projects, if they are mentioned at all: the answer is that many bodies are mentioned, but not sure about specific projects (Daan was actually not present in the 1st plenary meeting).
- EUDAT is there? yes, Jens Jensen is present.
- PROPOSAL by B. Jones: Prepare written material to propose an RDA working group, maybe through the existing forum. In case this working group is accepted we would need to participate in the next session **16-18 September** in Washington.

- Horizon2020: there are 2 public consultations where FIM should be mentioned.
  - Directions for ICT-driven public sector innovation in the EU:
    - identity management, personal data protection and data security.
    - Document & explanation: https://ec.europa.eu/digital-agenda/en/news/consultation-directions-ict-driven-public-sector-innovation-eu
  - Future research and innovation challenges in cloud computing, software and services: https://ec.europa.eu/digital-agenda/en/news/cloud-computing-software-and-services

Mikael Linden on behalf of Tommi Nyronnen proposes the **next meeting in CSC** (http://www.csc.fi/) the first week of **October**, exact date yet to be decided.

Meeting finishes at 12:54.

Appendix A

•**User friendliness** (high)
–Support for citizen scientists and researchers without formal association to research labs or univ

•**Browser & non-browser federated access** (high)

•**Bridging communities** (medium)

–Bridging is a central issue with an efficient mapping of the respective attributes

•**Multiple technologies with translators including dynamic issue of credentials** (medium)

•**Implementations based on open stds and sustainable with compatible licenses** (high)

•**Different Levels of Assurance with provenance** (high)

–Credentials need to include the provenance of the level under which it was issued

•**Authorisation under community and/or facility control** (high)

•**Well defined semantically harmonised attributes** (medium)

•**Flexible and scalable IdP attribute release policy** (medium)

–Bi-lateral negotiations between all SPs and all IdPs is not a scalable solution

•**Attributes must be able to cross national borders** (high)

–Data protection considerations must allow this to happen.

•**Attribute aggregation for authorisation** (medium)

–Attributes need to be aggregated from different sources of authority including federated IdPs and community-based attribute authorities.

•**Privacy and data protection** addressed with community-wide individual ids (medium)