

11-12-2014

Deliverable D9.4 (DS5.5.1)

Towards Horizon 2020 - The Enabling Users Experience

Deliverable D9.4 (DS5.5.1)

Contractual Date: 28-11-2014
Actual Date: 11-12-2014
Grant Agreement No.: 605243
Activity: SA5
Task Item: Task 5
Nature of Deliverable: R (Report)
Dissemination Level: PU (Public)
Lead Partner: SWITCH
Document Code: GN3PLUS14-557-118

Authors: Authors: Lukas Hämmerle (SWITCH), Ann Harding (SWITCH), Mikael Linden (CSC), Lalla Maria Laura Mantovani (GARR), Wolfgang Pempe (DFN), Mandeep Saini (DANTE)

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 605243 (GN3plus).

Abstract

This report provides an overview of the work and results of the GÉANT Enabling Users task in the Application Services Activity (SA5) in the first 18 months of the GN3plus project. The Enabling Users task is one of several tasks in the area of federated identity, supplementing the core eduGAIN service task. The scope of the Enabling Users task is to be an expert partner for research projects that have a need for federated identity management in a global context and to carry out a selection of pilots in collaboration with these research communities to improve their ability to use federated identity. A related goal is thereby to increase the practical use of eduGAIN, the interederation service created by GÉANT

<p>Deliverable D9.4 (DS5.5.1) Towards Horizon 2020 - The Enabling Users Experience Document Code: GN3PLUS14-557-118</p>

Table of Contents

Executive Summary	1
2 Introduction to “Enabling Users”	2
3 The “Enabling Users” Approach	3
4 Collaborations with Research Communities	6
4.1 CERN	6
4.1.1 Description	6
4.1.2 Use case	6
4.1.3 Collaboration objectives	7
4.1.4 Expected benefits	7
4.1.5 Achieved Results	7
4.1.6 Remarks	7
4.2 DARIAH	8
4.2.1 Description	8
4.2.2 Use case	8
4.2.3 Collaboration objectives	8
4.2.4 Expected benefits	9
4.2.5 Achieved Results	9
4.2.6 Remarks	9
4.3 ELIXIR	10
4.3.1 Description	10
4.3.2 Use case	10
4.3.3 Collaboration objectives	10
4.3.4 Expected benefits	10
4.3.5 Achieved Results	11
4.3.6 Remarks	11
4.4 European Space Agency (ESA)	12
4.4.1 Description	12
4.4.2 Use case	12
4.4.3 Collaboration objectives	12
4.4.4 Achieved Results	13
4.4.5 Remarks	13
4.5 GÉANT	13

4.5.1	Description	13
4.5.2	Use case	13
4.5.3	Expected benefits	14
4.5.4	Achieved Results	14
4.5.5	Remarks	15
4.6	Umbrella	15
4.6.1	Description	15
4.6.2	Use case	15
4.6.3	Collaboration objectives	16
4.6.4	Expected benefits	16
4.6.5	Achieved Results	17
4.6.6	Remarks	17
5	Basic eduGAIN Consultancy	19
6	Other Results	20
6.1	Dissemination of eduGAIN to scientific communities	20
6.2	Knowledge Data Base	20
6.3	Dissemination of GÉANT Data Protection Code of Conduct Know-How	20
6.4	Tools	21
6.4.1	isFederated Check	21
6.4.2	Test Identity Provider	21
7	Conclusions and Recommendations	23
Appendix A	Collaboration with other GÉANT Tasks	25
A.1	Service Activity 5: eduGAIN	25
A.2	Service Activity 5: Federation-as-a-Service (FaaS)	25
A.3	Joint Research Activity 3 (JRA3): Attributes & Groups Task	25
A.4	Network Activity 4 (NA4): User Identification & Liaison Task	26
A.5	Service Activity 7 (SA7): Support to clouds	26
References		27
Glossary		28

Executive Summary

While an increasing number of federations are becoming members of eduGAIN and its overall coverage is therefore growing, the various scientific communities stand at different starting points in the implementation and use of the federated identity management technologies it supports. On one hand proactivity on the part of AAI (Authentication and Authorisation Infrastructure) providers in understanding the needs of the scientific communities is highly desirable, while on the other scientific communities should develop their understanding of the benefits of federated AAI and what providers can be expected to deliver. The Enabling Users task aims to provide a key link between these research communities and eduGAIN.

This report highlights the work of the GÉANT Enabling Users task during the first 18 months of the GN3plus project. The task's main objectives are:

- To act as an expert partner for research communities wishing to use federated login as provided by the eduGAIN interederation service;
- To help enable several of GÉANT's own services for the use of eduGAIN;
- To build an eduGAIN knowledge database for sharing technical documentation focussed particularly on supporting the needs of user communities;
- To generally promote the increased use of federated login and eduGAIN.

Close collaborations with three European research communities, as well as basic support for several other communities, provided the task with a better understanding of the technical and organisational needs of these communities. Work on these complex use cases highlighted that many of the issues can be technically solved today, but the deployment of these solutions, as well as the decision-making process preceding it, often takes longer than expected. Many research communities also first need to familiarise themselves with the fundamental concept of federated identity management and today's authentication and authorisation infrastructures (AAI) before they can understand their advantages and limitations. This was also the case for the GÉANT project itself.

All parties involved found the collaborative and consultancy process to be beneficial, clearly showing that there is a demand for GÉANT to offer a permanent consultancy service of this kind.

1 Introduction to “Enabling Users”

GÉANT operates and develops eduGAIN, an inter federation service that enables users to securely use services from another country/federation. The eduGAIN service has grown significantly in coverage since it was launched in GN3, with 28 national federations represented on a global scale and an additional eight preparing to join. In addition, there are also two complementary tasks whose aim it is to increase the use of eduGAIN. One of these tasks, “Federation-as-a-Service” (Task 4, see [Appendix A](#)), builds a service to jump-start identity federations in countries or organisations where such an infrastructure does not yet exist. This increases the breadth of coverage of eduGAIN. By contrast, “Enabling Users” works directly with research communities to address their challenges in using federated identity management, thereby increasing the depth of use of eduGAIN.

Most task members are directly responsible for running a national NREN identity federation, such as IDEM in Italy, DFN-AAI in Germany, HAKA in Finland, FER in France and SWITCHaai in Switzerland, and have participated in eduGAIN since the time when the service was in development. Others are responsible for deploying and operating federated services and are therefore expert in the field of federated identity management.

The main objective of the “Enabling Users” task is to act as an expert partner for large pan-European projects with AAI requirements. The task’s method is to collaborate with large international user communities through two or three well-defined, replicable use cases that benefit the wider research and education community. The intention is to increase the practical use of eduGAIN, while extending inter federation technology and AAI functionalities based on real user requirements.

International research communities in particular benefit from eduGAIN because their members are working at different institutions located in different countries. Thanks to eduGAIN, users can access the services of one or more research communities through their home institution user account. Research projects that enable their services for eduGAIN also benefit from the existing legal and technical framework it provides.

Building on the experience of the pilots, a related objective is also to create a knowledge database that would allow research communities and other potential users of eduGAIN to inform themselves on the technical and organisational aspects of running services in eduGAIN.

Last but not least, the use of eduGAIN within the GN3plus project itself was to be increased, the GÉANT community being a good example of a pan-European virtual organisation with advanced federated identity requirements.

2 The “Enabling Users” Approach

The requirement for fine-grained access management for research data has become a major issue in science. In 2012, a cross-section of e-Research projects and infrastructures, driven by the interest in using federated identity management technologies, produced a paper entitled ‘Federated Identity Management (FIM) for Research Collaborations’ [FIM4R]. This paper detailed requirements for the usage of federated access from various e-Research communities and identified issues that pose challenges for the wider adoption of FIM technologies offered by national federations and by eduGAIN. The Enabling Users task was created to respond to the issues addressed in the paper, which was used as a basis to define the potential work area.

Scientific communities stand at different starting points in the implementation and use of the federated identity management technologies offered by well-established AAI providers such as GÉANT’s eduGAIN inter federation service. Proactivity on the part of AAI providers in understanding the needs of the scientific communities is highly desirable, while scientific communities should develop their understanding of the benefits of federated identity management and AAI and what providers can be expected to deliver. The Enabling Users approach therefore involves becoming a collaborative partner of research communities to actively help them make use of AAI technologies.

The GÉANT participants in the Enabling Users task were able to benefit from their previous close contacts with several of the research communities engaged in FIM4R, as these had often required the specific networking services that GÉANT could provide. However, direct participation in the FIM4R forum and, later on, in the RDA FIM Interest Group [[RDA-FIM](#)], also proved invaluable towards identifying and sharing progress on collaborative pilots.

In order to address complex requirements in sufficient depth, yet help as many communities as possible within the limited two-year period, the planned work was divided into two focus areas:

- Close collaborations with three communities on their three respective use cases, for which extended pilot support was provided.
- Basic eduGAIN consultancy for all communities interested in Enabling Users and eduGAIN.

The experience and know-how gained from the pilots and by providing consultancy to several research groups contributed towards building the knowledge database, which was another goal of the task.

As the goal was to work on two or three use cases in a close collaboration, suitable cases had to first be identified and refined based on the technical issues set out in the FIM4R paper. To find suitable use cases, at the FIM4R meeting in March 2013 at the Paul Scherrer Institute (PSI) in Villigen (Switzerland),

the Enabling Users team invited all research groups to submit their use cases for collaboration. This invitation was announced alongside one from REFEDS, which was also looking for similar use cases. The invitation was sent to both the REFEDS and FIM4R mailing lists to widen the scope. The Enabling Users team was primarily looking for use cases from mostly European research communities, while REFEDS was also interested in use cases from non-European research communities. Both parties (Enabling Users and REFEDS) coordinated their work so as to maximise the support that could be offered, and shared their experiences as the pilots progressed.

The use cases were collected in GN3plus Y1, i.e. between March and May 2013, using an online form in which submitters were asked to provide (among other things) a use case description, existing SAML know-how, contact information, non-browser requirements, organisations involved and user base, time constraints, and how much time the project could contribute to a collaboration with the Enabling Users task. By mid-May 2013 a total of 11 use cases had been submitted by research groups from a wide variety of disciplines (oceanography, climatology, seismology, biology, language research and physics) and including both web and non-web requirements. The large number of use cases submitted as well as the wide range of scientific communities involved can be considered as a clear sign of the interest and demand for services such as Enabling Users providers.

Each use case was evaluated on the basis of consistent criteria including timing constraints, reusability by other communities, available know-how and resources, feasibility, and size and distribution of the community, as well as other aspects such as GÉANT user liaison priorities. For example, some research projects submitted use cases even though they were not active in the same time period as Enabling Users, in which case they were considered for future support. The result of the evaluation was then to start close collaborations to work on the use cases of the following three research communities:

- DARIAH-DE: Arts and humanities research
- ELIXIR: Life science research
- Umbrella (CRISP/PaNdata): Large photon / neutron research

This decision was first announced to the selected research communities, then to those that had not been selected for a close collaboration at this time, and finally to the public via the FIM4R and REFEDS mailing lists. The availability of ongoing eduGAIN support for those not engaged in pilots was also explicitly highlighted as well as the prospect that work on additional use cases could start in a later phase of the GN3plus project.

Based on progress of these pilots and available resources, two additional close collaborations were started at beginning of year 2 of GN3plus, with the following research communities:

- CERN Worldwide LHC Computing Grid (WCLG): High energy physics research
- ESA Earth Observation research

Besides the close collaborations on the use cases of the five above-mentioned research communities, the Enabling Users task also provided basic eduGAIN consultancy to other research communities upon their request. This basic consultancy comprised:

- Responding to general inquiries about eduGAIN and FIM in general.

- Referral of the communities to appropriate eduGAIN/federation contacts in countries where they are mostly active.
- Attendance at meetings where eduGAIN/FIM was a topic in order to advise them.
- Providing research communities with an overview of different architectural and technological choices regarding FIM.
- Recommending software and technologies to help solve research communities’ needs.

3 Collaborations with Research Communities

The following communities and their use cases are listed in alphabetical order. The GÉANT project is also included as it is a community on whose use cases and services Enabling Users have been working.

3.1 CERN

3.1.1 Description



CERN, the European Organization for Nuclear Research [[CERN](#)], is active in high-energy physics research. It is well-known for its Large Hadron Collider (LHC), the world's largest and most powerful particle accelerator. The Large Hadron Collider has four main particle detectors that analyse the results of particle collisions. A large community consisting of over 10 000 physicists from more than 60 countries collaborate to process the huge amount of data the detectors generate. Most of these scientists, who are located all over the world, require remote access to the data that these experiments generate.

3.1.2 Use case

CERN, and in particular the large Grid community affiliated to it, has been successfully using an authentication and authorisation infrastructure based on X.509 certificates for years. This infrastructure ensures a high level of trust and allows fine-grained authorisation. Non-browser applications are well-supported using certificates. CERN users would benefit from a system that allowed them to use their CERN credentials (e.g. an X.509 grid certificate) to log in to web-based services. At the same time, it would benefit other researchers to be able to use their federated university account to access CERN services via eduGAIN without the need for a X.509 certificate, which can be complicated to install and use.

Some services offered by CERN contain sensitive research data or only allow certain actions to be performed by specifically authorised users. Should a user's identity be compromised, action must be taken in a coordinated and determined way. CERN's experience gained from operating the computing grid has led them to establish best practices guidelines for handling such security incidents. As those guidelines were created specifically for the grid community, and not for a federated identity environment such as that which eduGAIN operates, CERN proposed and requested that similar guidelines and policies should be codified for eduGAIN.

3.1.3 Collaboration objectives

The Enabling Users Task helped CERN to:

- Connect ADFS-based identity management via the Swiss identity federation to eduGAIN. This would allow bilateral access to and from CERN services and identity providers operated in eduGAIN.
- Contribute to formulating a new policy for a more formalised incident handling in eduGAIN, which could be in part derived from work previously done by the Security for Collaborating Infrastructures (SCI) group.

3.1.4 Expected benefits

The main benefit for CERN employees will be the possibility of using their CERN user account to access and use web services operated by universities and research institutions via eduGAIN. At the same time, CERN collaborators could use the user account issued to them by their home institution to access some of CERN's web services. Also, eduGAIN can benefit from the profound know-how gained by the Grid community around CERN in the past years in terms of handling security incidents and level of assurances in a distributed infrastructure, which complements the experience of the NRENs in the CERT environment.

3.1.5 Achieved Results

- Users can now access several CERN services (e.g. INDICO, a tool for the management of complex conferences, workshops and meetings) using federated login via eduGAIN.
- Some CERN staff members are able to access eduGAIN services via federated login.
- Preliminary discussions have already begun between experts of the Grid and identity federation communities for the definition and deployment of a (security) incident handling policy.

3.1.6 Remarks

CERN has been operating an ADFS-based single sign-on solution for several years. Therefore, it was agreed to integrate this existing infrastructure into eduGAIN in a bilateral way. Even though ADFS-based SAML entities have already been successfully used in several identity federations, ADFS entities usually act either as a Service Provider or as an Identity Provider. CERN's ADFS entity has however been operated for years as both a Service Provider and Identity Provider sharing the same identifier. In addition, Microsoft's SAML implementation lacks certain features (such as handling of SAML metadata containing multiple entities, accepting the same certificate for multiple entities and generation of persistent ID attribute as attribute) that Shibboleth and SimpleSAML PHP – the two most used SAML implementations in the academic world – support already. These factors made integration of CERN's ADFS-based solution into an existing federation and eduGAIN challenging from a technical standpoint.

3.2 DARIAH

3.2.1 Description



DARIAH stands for Digital Research Infrastructure for the Arts and Humanities [DARIAH] and "is a network of people, expertise, information, knowledge, content, methods, tools, and technologies coming from various countries."

This ESFRI project aims to investigate, explore and support work across the broad spectrum of Digital Humanities and, among other things, provides a virtual research infrastructure to be used by eHumanities projects. Currently there are over 2000 users registered with the user management of DARIAH. It is assumed that many more users will use DARIAH's services once these are fully available at a pan-European level.

3.2.2 Use case

Among research communities, the need for federated access to services is seen as an essential success factor. There are particular benefits in the Social Sciences and Humanities (SSH) sector, where users may vary widely in their levels of technical proficiency and just need quick and easy access to web-based electronic research tools. The experiences of research communities with grid computing showed that X.509 certificate-based infrastructures presented a major obstacle to having those research tools adopted by the wider community. Thus federated identity management is seen as the only acceptable authentication and authorisation technology for the SSH community.

The FP7/ESFRI programs of the European Commission (EC) have led to the creation of long-term, Europe-wide research infrastructures, which need to interfederate to manage virtual organisations that include members from different countries. eduGAIN's inter federation service provides an answer to this need. Academic research projects often operate their services in different countries, with many of these services requiring authentication and authorisation scaling beyond national or organisational boundaries. Currently, these services often only use local or national authentication and authorization and are limited in terms of where they can be delivered or are required to introduce user management overhead..They could therefore benefit from integration into eduGAIN. Enabling eduGAIN inter federation support for these services requires a certain know-how and effort on the part of the service operator. Given that the services operated by SSH communities are more widely distributed and probably greater in number than those of many other research communities, and given that the number of their services is likely to increase further, the challenge lies in demonstrating that research projects like DARIAH can efficiently add their services to eduGAIN.

3.2.3 Collaboration objectives

The Enabling Users Task agreed to support DARIAH with:

- Enabling federated access to all DARIAH services.
- Connecting to eduGAIN, i.e. making DARIAH services available to users from all participating federations.

- Enhancing attribute release by supporting the adoption of the GÉANT Data Protection Code of Conduct for Service Providers in EU/EEA in the relevant federations.

3.2.4 Expected benefits

DARIAH users and researchers from the SSH community will be able to conduct their research within a pan-European federated environment based on AAI and supporting Single Sign-On. Other ESFRI projects in the fields of humanities and social sciences, such as CLARIN and CESSDA, which have similar requirements and aims could re-use the solutions developed for and together with DARIAH.

3.2.5 Achieved Results

- Enabling Users identified and elaborated three possible options to enable DARIAH to join eduGAIN [[GN3PLUS13-642-23](#)]:
 - A – Adding Services via an Existing Federation;
 - B – Creating a New Federation;
 - C – Joining via a Proxy (either SAML IdP Proxy/Hub or Web Proxy).
- After several discussions and meetings, DARIAH decided for option A (adding services via an existing federation) in the medium term, while their community considers whether option B may be a long-term option.
- Eight DARIAH SPs and the DARIAH Homeless IdP were exported to eduGAIN (via DFN-AAI).
- All these entities adopted the GÉANT Data Protection Code of Conduct (CoCo).
- Enhanced collaboration plan to identify and carry out additional work around attributes and groups, which is not covered by the current DARIAH project schedule, in order to support the use case (ongoing work).

3.2.6 Remarks

The DARIAH community is similar to other digital humanities communities, such as CLARIN or CESSDA. All these communities comprise of a large number of researchers in different European countries. The number of (web-based) services that each of these communities operates is generally larger than is the case for the other research communities with which Enabling Users collaborated.

Unlike other communities, DARIAH (more specifically DAASI, the company that was contracted by DARIAH) already possessed a comprehensive and rather advanced know-how in the area of federated login and SAML. The German DARIAH-DE community also had previously operated several services that allowed federated login. Additionally, a central group management system was already available.

Despite this considerable advantage, DARIAH still benefited from the collaboration, especially the work on determining which options were available to first add the DARIAH services to an existing identity federation and then enable these services for eduGAIN. This work has also been appreciated by other communities, especially as these options for adding services to eduGAIN were not previously clear to all.

3.3 ELIXIR

3.3.1 Description



ELIXIR [ELIXIR] is building a sustainable European infrastructure for biological information, supporting life science research and its translation to medicine, agriculture, bio industries and society. In May 2014, the Council of the European Union elevated it to one of the three prioritised ESFRI projects.

3.3.2 Use case

Many of the datasets in life sciences cannot be freely distributed due to ethical, legal, societal or intellectual property reasons. Processing of the larger datasets also requires computing capabilities that are not freely available. These services require sufficiently reliable authentication and proper authorisation.

The European Genome-phenome Archive (EGA) is a service of the European Bioinformatics Institute (EBI). The EGA provides permanent archive and data dissemination services for all genetic and phenotypic data; study participants have signed an informed consent agreement authorising data release only for a specific research use or to bona fide researchers, thus preventing fully public data dissemination. Data access is granted by a Data Access Committee (DAC), which is typically formed from the same organisation that monitored the original data collection and analyses, or by a designate of this organisation. ELIXIR has developed a Resource Entitlement Management System (REMS) tool to manage the data access application process.

3.3.3 Collaboration objectives

The collaboration objectives for ELIXIR were to:

- Make the EGA portal service provider available via eduGAIN, providing the quality and functionality required by ELIXIR.
- Make the REMS service provider available and functional via eduGAIN.
- Minimise the number of homeless users, i.e. users with no institutional identity provider, needing access to EGA (estimated at around 4000 users).
- Identify ELIXIR's requirements in terms of Level of Assurance (LoA) mapped against known potential solutions.
- An additional optional goal was to make a generic federated version of REMS available as a test instance for other projects that might be interested in this tool.

3.3.4 Expected benefits

The following benefits are expected for the ELIXIR research community as well as others in the bioinformatics field:

- The integration of the EGA portal will develop the SAML/AAI know-how of the ELIXIR collaboration and provide a working example of a bioinformatics SP.
- Exploring the issues facing data access management with ELIXIR will improve the current state of the art around issues such as support for LoA and group workflow management.
- The requirements of ELIXIR provide a trigger to increase the availability of identities via eduGAIN.

3.3.5 Achieved Results

The goals that were achieved include:

- REMS and EGA SPs were exported to eduGAIN.
- ELIXIR studied the LoA offer of existing federations and decided that the key requirements for a minimum LoA level are that:
 - An account belongs to an individual (i.e. there are no group accounts);
 - The home organisations have a standard identity vetting process;
 - Accounts are closed when the individual leaves the home organisation.
- Based on the survey of the federations:
 - SWITCHaai (CH), Haka (FI), Edugate(IE), DFN-AAI(DE), IDEM(IT), SURFconext federation(NL) and Fédération Education-Recherche (FR) were found to meet the requirements;
 - UK access management federation (UK) and, outside Europe, InCommon (US) did not meet the requirements fully.
- REMS was configured to rely on the Identity Providers in the federations who met the requirements.
- Although verifying that the Home Organisations were willing to release attributes to the SPs was not within the scope of the project, REMS nonetheless committed to the GÉANT Data Protection Code of Conduct (CoCo) so as to encourage the Home Organisations to do the same.

3.3.6 Remarks

Unlike in the case of the DARIAH-DE community, only two ELIXIR services were candidates to bring to eduGAIN, and the Level of Assurance (LoA) of the users accessing them is more important than the SSH sector use case.

Unfortunately, exactly those countries (and their federations) with the largest ELIXIR user base have few rules or policies regarding the quality of identities and authentication for federated users, reflecting perhaps cultural and organisational differences operating at a higher level than research and education. Therefore, the UK and the US federations have not yet been granted access to authenticate at EGA and REMS via federated login, and a strategy for moving forward with identities from these countries will need to be developed. Moreover, some of those organisations whose users can authenticate for the ELIXIR services via federated login may not release the necessary attributes. Therefore, Home Organisations need to be convinced to release attributes to the ELIXIR SPs, ideally based on a generic rule that releases the required attributes if an SP supports the GÉANT Data Protection Code of Conduct (CoCo).

During the collaboration with the Enabling Users group, the ELIXIR project established an AAI task force that is currently designing its authentication and authorisation infrastructure.

3.4 European Space Agency (ESA)

3.4.1 Description



The European Space Agency [ESA] is Europe's gateway to space. Its mission is to shape the development of Europe's space capability and ensure that investment in space continues to deliver benefits to the citizens of Europe and the world. ESA is an international organisation with 20 Member States.

One of ESA's branches is Earth Observation (EO). Data from the many instruments on board ESA satellites, and from more than 20 non-ESA Earth Observation satellites, are sent to a network of worldwide acquisition stations, processed in these stations or at archiving centres, and then distributed via the use of ESA EO web application services to a worldwide user community that includes around 20 000 scientists. The Earth Observation Single Sign On system (EO-SSO) is already in place to provide Single Sign On functionalities and login to its Web applications.

3.4.2 Use case

This use case aims to prepare the ground for the ESA to join eduGAIN by interconnecting existing and future ESA SPs to eduGAIN, as well as to make Earth Observation data products and services available to a wider scientific community. In addition, interconnecting the existing ESA IDP to eduGAIN would allow ESA users to access federated services provided by research partners participating in current and future projects. The outcome of this pilot is of particular importance in view of its possible applications within the context of the ESA/EU Copernicus program.

The use case aims to gather an understanding of what is required to fulfil both the technical and administrative requirements for the ESA EO AAI framework to be fully compliant with eduGAIN.

The use case consists of three work packages:

1. Deployment of a test environment reproducing the Landsat data dissemination server as Service Provider in the eduGAIN interederation.
2. Deployment of a test environment reproducing the ESA EO Identity Provider in the IDEM test federation, fulfilling all the technical compliance requirements to be admitted in the production IDEM Federation and in eduGAIN.
3. Consolidation of the administrative documentation required to enable the submission of a formal, fast-track application to IDEM/eduGAIN for federation membership as well as of a successful application for future services.

3.4.3 Collaboration objectives

The collaboration objectives for ESA are:

- ESA SPs data should be made available to selected IDEM/eduGAIN research organizations.
- IDEM-test services should be made available to the ESA test IdP users (Test services to be agreed with IDEM e.g. between file exchange, virtual box, eduroam, etc.).
- The ESA IdP profile harmonisation should be prepared for IDEM/EDUGAIN with release of recommended attributes.
- User distinction between researchers and non-researchers (e.g. ESA homeless), achieved via a suitable utilisation of the “affiliation” attribute.
- Compliance of SPs with the GÉANT Data Protection Code of Conduct.
- Administrative documents drafted for joining IDEM/eduGAIN validated by IDEM/eduGAIN, so that applications for further services can be easily submitted.

3.4.4 Achieved Results

As this use case has just started at the time of writing in October 2014, results are expected for the beginning of 2015.

3.4.5 Remarks

The ESA’s Earth Observation Department is based in Italy. For this reason the local identity federation that will register the Identity Provider and the Service Providers will be the Italian IDEM federation. ESA, however, is outsourcing its systems to Siemens Romania. Therefore, in order to ensure the success of the use case, the technical personnel located at this external facility had to be provided with a clear, quick knowledge guide and step-by-step implementation checklist.

3.5 GÉANT

3.5.1 Description



GN3plus, known simply as GÉANT, is the extension of the third term of the successful GÉANT networking project [[GÉANT](#)], which is in itself a European infrastructure and research project. Co-funded by the European Union (EU) and Europe’s National Research and Education Networks (NRENs), GÉANT seeks to promote the free, unimpeded movement of scientific data and knowledge, by connecting and empowering research and education (R&E) communities within Europe and other world regions. By driving knowledge creation as the global hub for research networking excellence, GÉANT’s vision is to become the unified European Communications Commons.

3.5.2 Use case

With over 250 participants from more than 40 organisations all over Europe, requiring access to various different services for their day-to-day work, GÉANT evidently has federated identity management needs of its own. For example, the video conference directory service (eduCONF), its collaboration platform (GÉANT Intranet), its network performance-monitoring infrastructure

(perfSONAR), its dynamic bandwidth provisioning service (BoD) and its ticketing system (OTRS) all need to know the users before they can be given access. Therefore, authentication and authorisation is required for these services, and previously end users were typically issued different sets of credentials for each service. This resulted in a lot of overhead work because service administrators had to manage a large number of user accounts. The users, on their part, would have to juggle multiple usernames and passwords.

One goal of the Enabling Users task was therefore to enable federated login via eduGAIN for several of these services, or to provide the service operators with sufficient technical expertise and assistance to allow them to enable federated login themselves. This included:

- Providing support in assessing AAI/eduGAIN requirements for GÉANT services.
- Providing a single point of contact for all GÉANT services to address both authentication and authorisation needs.
- Enabling federated login for GÉANT services using eduGAIN.
- Providing a centralised group management system for GÉANT Services.

3.5.3 Expected benefits

The primary benefit for the end users is the ability to use the credentials issued by their home organisation to access the GÉANT services that support federated login, reducing the need for additional passwords. When NRENs change staff, they do not have to carry out additional steps to remove users from GÉANT services. For operators of GÉANT services, one benefit lies in the reduced efforts in terms of user management and password problems. The risk of out of date user information is minimised and security is more easily managed as communication is via the identity provider only. In addition, the prospect exists in the future for a GÉANT group management solution that will enable a more fine-grained access control, as users will be able to be identified across all services thanks to their federated identity.

3.5.4 Achieved Results

The following results were achieved:

- A workshop was held during the GN3plus Symposium 2013 to collect the AAI/eduGAIN use cases from the community, resulting in the definition of a prioritised list of services to be integrated with eduGAIN during the lifetime of the GN3Plus Project and in increased awareness of the utility of AAI across the project.
- Consultations were given to various GÉANT Services (e.g. perfSONAR, BoD, OTRS, eduCONF) to help address their authentication and authorisation needs.
- During Year 1 of GN3plus, federated login was enabled for following services:
 - GÉANT Intranet: A SharePoint-based collaboration platform for all GÉANT project participants;
 - Partner Portal: A portal for NRENs to order and access information on products and services;
 - AutoBAHN: Automated Bandwidth Allocation across Heterogeneous Networks;

- eduCONF: A global directory service for videoconferencing systems.
- In Year 2 of the project, the current status of ongoing work is as follows:
 - Federated login has been enabled for:
 - The Product Management Lifecycle Portal (PML Portal);
 - eduPERT Intranet; and
 - Cloud Settings.
 - Federated login has been enabled in test infrastructure for:
 - perfSONAR;
 - OTRS.
 - Work is in progress on the GÉANT Group Management System.

3.5.5 Remarks

Enabling federated login via eduGAIN for the GÉANT Intranet was the most challenging but also the most important work as it was the stepping stone towards also enabling federated login on several other services on the same platform. This result was very well-received by GÉANT participants and was a very popular and beneficial development both for GÉANT IT and the end users. This project also helped promote the benefits of eduGAIN Integration to the community, and as a result SA5 is receiving an increasing number of use cases for federated login.

Once the few remaining issues, such as attribute release policy and some security concerns (e.g. email spoofing etc.), are resolved, the GÉANT community will be able to use federated login to access all GÉANT Services with a single set of credentials issued and managed by their home organisation, while access control and authorisation will be retained by the individual GÉANT services.

3.6 Umbrella

3.6.1 Description



Umbrella is the pan-European authentication and authorisation platform for the photon and neutron research community operated by several FP7 projects, and mainly by CRISP and PaNdata. Umbrella's partners are for the most part European large photon and neutron facilities, plus some additional facilities such as the heavy-ion project at GSI, Darmstadt. A total of more than 30 000 users visit these facilities annually, with between 40%-60% of these, depending on their sector, visiting multiple facilities where they first have to be registered and issued an identity. The purpose of Umbrella is to provide these users with a single identity that simplifies the registration overhead. This common Umbrella identity also allows them access to research data at the facilities or to perform research experiments remotely.

3.6.2 Use case

The use case consists of two independent work packages:

- Bridging of eduGAIN-Umbrella.
- Non-browser access to facility servers.

Users of the Umbrella partner facilities are often from universities, therefore most of them already have a university identity that allows them to access various federated services. Linking their university identity to an Umbrella identity allows them to access Umbrella services by signing in with their university identity.

At present, experimental work often requires researchers to visit a facility in person. This results in much time and costs spent for travel and accommodation. For certain experiments, or for accessing the data produced by experiments, the need for this physical presence could be obviated by enabling researchers to access a facility's control and data servers remotely. This requires non-web access (e.g. via SSH), ideally using the identity and credentials issued by the researcher's home institution. Both requirements can be addressed by Moonshot, a unifying federated identity management technology developed by Janet and piloted on a pan-European basis in GÉANT.

3.6.3 Collaboration objectives

The objectives that were agreed on with the Umbrella community are:

- An outline of a proposed architecture for bridging eduGAIN and Umbrella.
- A demonstration of a working bridging between eduGAIN and Umbrella on a national scale at Paul Scherrer Institute (PSI).
- A rollout of eduGAIN/Umbrella bridging to four other facilities.
- A scope definition for Moonshot deployment at PSI – service, affected infrastructure, etc.
- An architecture outlining deployment of Moonshot at PSI.
- A demonstration of a working Moonshot-enabled SSH access with X-Forwarding.
- A plan for an international demo of Moonshot SSH and further Moonshot deployment as needed.
- Bridging federated identities and Umbrella identities.

In short, the goal was to enable university researchers to access Umbrella services using their university identity. In order to implement this, the Umbrella platform had to be extended by a bridge that links eduGAIN identities to Umbrella identities. In a later phase, the bridge could also allow Umbrella users to access eduGAIN-enabled services using their Umbrella ID.

An additional goal was to build a small Moonshot infrastructure (a Moonshot Identity Provider, Service provider and optional Trust Router) to support the use of SSH with X-Forwarding for remote experiment access via federated identity.

3.6.4 Expected benefits

For the Umbrella community, one benefit is the potential usage increase of Umbrella that could result by lowering the barrier for researchers to use Umbrella services by allowing them access via eduGAIN.

Being enabled to use their organisation's account, university users will not need to register a new Umbrella identity to use its services.

Becoming familiar with Moonshot, and eventually running Moonshot services, is a first step towards making it possible to conduct remote experiments and access research data without the need to be physically present at the facilities.

3.6.5 Achieved Results

Whereas the technical objectives set out were easily achieved and demonstrated, there are political and strategic questions that first need to be discussed within the Umbrella and eduGAIN communities before a wider production deployment can be planned. Therefore, in particular the following two objectives (and dependent objectives) remain open:

- Umbrella users accessing eduGAIN services: The bridging currently works only in one direction. Allowing Umbrella users to access eduGAIN services was less of a priority for the Umbrella community. In addition, as Umbrella includes researchers from commercial companies, a policy discussion regarding their accessing services that are primarily reserved for the higher education & research community needs to take place. The question as to whether this should be accepted or not has yet to be discussed in the eduGAIN community.
- Deployment of the eduGAIN bridging to four facilities. While the bridging from eduGAIN to Umbrella as well as a basic Moonshot setup were implemented and successfully tested, the facilities that operate Umbrella together have postponed the decision as to whether or not to introduce the Umbrella-eduGAIN bridge and Moonshot support in September 2014 due to other internal organisational commitments.

3.6.6 Remarks

From eduGAIN's point of view, the Umbrella system only consists of a single Service Provider and potentially, at a later stage, one Identity Provider. Thanks to the bridging, attribute release to the system is likely to be less of an issue, however the bridging also adds complexity. While technical solutions often can be found and implemented relatively quickly, political and operational decisions in the end are what decide whether this solution is deployed or not. Getting different parties to reach a consensus to make such a decision often takes more time than expected. Therefore, even though the pilot collaboration was generally held as very positive and valued by both parties, the eduGAIN bridge could not yet be deployed in the production Umbrella system. The same is also true for the Moonshot component.

One difficulty observed with the Moonshot work package was that, at the time when the Umbrella community was starting this work, the Moonshot documentation was still in a very early stage of development. The documentation was either very detailed (RFCs) or too high level for Moonshot service deployment. Even though the Moonshot developers provided valuable inputs and assistance on request, the documentation provided was still in development, which meant that it was difficult for the Umbrella maintainers to deploy Moonshot services and to become familiar with the technology from a technical point of view. This was a particular challenge because the deployment of Moonshot requires multiple skill sets related to several technologies that are already complex in themselves.

Based on feedback from this initial trialling, the Moonshot documentation has been significantly improved to the benefit of later pilot deployers.

4 Basic eduGAIN Consultancy

In addition to the close collaboration with the above-mentioned research communities, as well as with GÉANT itself, the Enabling Users team also looked to deliver support and provide an ongoing point of engagement for research communities. In order to achieve this, the team provided basic consultancy to several other research communities. Most of these communities contacted the Enabling Users team of their own accord, while others were referred to it by the NA4 User Liaison team (see Appendix A).

Basic consultancy included:

- Introductions to federated identity management, SAML and eduGAIN.
- Advice in strategic decision-making and planning for AAI/federated identity implementations.
- Referrals to local identity federation operators.
- Help in registering existing federated services with eduGAIN.
- Assistance in problem finding and debugging.
- Recommending user interface improvements for a better user experience.
- Support for applying the GÉANT Data Protection Code of Conduct.

In the 18 months since the GN3plus project started, basic consultancy has been provided to the following research communities and services:

- DASISH (CLARIN/CESSDA): Social Sciences and Humanities research.
- European Integrated Data Archive (EIDA): Seismic research.
- neuGRID N4U: Neuroscience grid service portal.
- ESA (European Space Agency) prior to transition to a full pilot, now in its early stage at the time of writing.

This basic consultancy provided valuable inputs on the requirements and AAI needs of other research communities. It also helped to increase the AAI know-how and the general awareness of federated identity management within these communities, which in the case of ESA resulted in a close collaboration and a pilot project.

5 Other Results

5.1 Dissemination of eduGAIN to scientific communities

Spreading the word about eduGAIN is important to increase awareness among potential users of the benefits and opportunities the service offers. Therefore, the Enabling Users task has attended several meetings, workshops and conferences in order to present and discuss eduGAIN. In particular, task representatives gave presentations at two FIM4R events, a VAMP meeting, a REFEDS meeting, and a DASISH workshop and strategy meeting.

5.2 Knowledge Data Base

Part of the work of the Enabling Users task included the creation of a knowledge database so that federation operators and administrators of eduGAIN-enabled services can access and exchange information on various (mostly technical) topics that are relevant to the operation of eduGAIN services. The database was set up with the help of the eduGAIN task in Q2 2013 and is now available as a wiki [[Wiki eduGAIN](#)]. It is a fully eduGAIN-enabled service and was designed to provide a good example of such a service, e.g. by supporting the GÉANT Data Protection Code of Conduct and by being a tolerant attribute consumer, only requesting the minimum necessary attributes for an authorisation decision.

The wiki can be read by everyone, while all users who can authenticate via eduGAIN and be uniquely identified can modify content. Content in the knowledge database has been structured to best serve a particular group of users (federation operators, SP admins, IdP admins) in supporting eResearch's use of federated identity. Content continues to be created on-demand when research groups need specific information.

5.3 Dissemination of GÉANT Data Protection Code of Conduct Know-How

One major issue encountered in the first phase of eduGAIN is the insufficient attribute release of Identity Providers to eduGAIN-enabled services. One underlying reason why Identity Providers often do not release the required attributes about their users to a service is the presence of data privacy concerns. This issue is even more serious when users wish to access services operated in another country and thus another jurisdiction. One solution developed during the GN3 project for this problem

is the GÉANT Data Protection Code of Conduct (CoCo,) that can be committed to by services operated in EU countries or countries with similar data protection laws, and signalled in metadata, thereby allowing release decisions to be automated. In order to accelerate the adoption of the CoCo and gain more experience in its application, the Enabling Users team fostered its use for its own services (e.g. the eduGAIN wiki) and for services it has assisted to become eduGAIN-enabled (e.g. DARIAH services), as well as for services in the local federations where the Enabling Users participants are part of the federation operator team (e.g. GARR Wifi service). By actively helping to apply the CoCo to services, improvements in its documentation and development, as well as of its related services (e.g. the CoCo monitor), can be fed back to the eduGAIN task, which is responsible for its ongoing maintenance..

5.4 Tools

During work with the research communities on their use cases it became apparent that they could benefit from two supporting tools that would enhance the use of eduGAIN and save much manual work, as described below.

5.4.1 isFederated Check

The first two questions that a research community considering enabling their services for eduGAIN needs to ask are: a) At which organisations are its users? and b) Are their organisations already federated and eduGAIN-enabled? Most of the time they have the data to answer the first question but not the second. The isFederated Check is a web service [[isFederatedCheck](#)], which provides a list of email addresses, domain names or URLs to match organisations that are already part of an identity federation and in the eduGAIN metadata. The output of the tool is a list and summary of all identified organisations specifying their status as to whether they are federated and eduGAIN-enabled. For those that are not, it provides a direct link to the federation operator or the organisation's technical contact. The isFederated Check covers all production and almost-production identity federations worldwide. As well as other features, the isFederated Check also includes a REST/JSON interface, which was requested by several federation operators. The interface can be queried to obtain results in a format that is better suited to be processed by other web services. Initially announced as a Beta service, the isFederated Check was improved thanks to feedback from the community and is stable since September 2014.

5.4.2 Test Identity Provider

While assisting research groups and operators of cloud services to enable their services for eduGAIN, it was discovered that some have difficulties in testing federated access to their own services. This is because Service Provider administrators do not always have a federated account that allows them to access their own service via eduGAIN. This is especially true in the case of commercial cloud providers who normally do not have nor can easily obtain an account with a university IdP participating in eduGAIN. Often SP administrators do not operate an Identity Provider of their own that would allow them to test the federated login to their own services.

In order to resolve this, the Enabling Users team have been developing an eduGAIN Test Identity Provider to allow any administrator of an eduGAIN Service Provider to test access to his own service. The Test Identity Provider ensures that administrators can create test user accounts that can only be used to access the SP administrator's own service.

At the time of writing of this report in October 2014, a first alpha version of the eduGAIN Test Identity Provider was being tested by the Enabling Users team.

6 Conclusions and Recommendations

The ideal scenario would be for GÉANT to be able to provide pan-European research groups with a catchall out-of-the-box solution which immediately addresses all their cross-border needs. However, the experience from pilots suggests that unfortunately this is often not possible. Although the requirements of different research groups at first glance may appear to be similar or at least related, the details and focus of the specific use cases often vary greatly. These differences are often what provides the greatest value to the end users of a particular service, and therefore care has to be taken to respect them. A possible promising alternative being considered involves additional services being layered on top of eduGAIN. Some of these, such as VO Platform as a Service or Affiliation checking services are being developed with a view to operation at a GÉANT or federation level. The intent is to benefit from the experience of those federations that already offer these advanced services on a national level, but to scale the service to serve cross-border communities. In other cases, consultancy is recommended to continue to help research communities embed any highly specific niche requirements in their own systems under their own control. In this way, each level of the infrastructure preserves the trust relationship that is so important when delivering services to the end user.

For some research groups, a high Level of Assurance (LoA) within their limited group of users is fundamental (ELIXIR), while for others a wide coverage with a good attribute release is more important (DASISH); others still already have and require fairly advanced group management tools (DARIAH), while others may not need fine-grained group management at all (Umbrella). Applying all these features uniformly to the full infrastructure for the benefit of some would greatly increase the costs and complexity for others in the delivery chain and therefore damage the value proposition of eduGAIN as a general infrastructure. In particular, the costs of enhancing the service uniformly with advanced features can often fall in disproportionate measure on the campus IdP administrators, who typically have no clear access to research infrastructure funding to meet them. The business and cost recovery aspects of federated identity for eResearch therefore require further study.

Issues that are mentioned in the TERENA AAA Study [\[AAA\]](#) and in the FIM4R paper were also confirmed by the experience of the Enabling Users team. These include:

- The need for stronger authentication and identity vetting (ELIXIR/CERN).
- Insufficient attribute release (DARIAH, CLARIN) by Identity Provider.
- The general lack of campus IdPs exported by federations into eduGAIN in the early years of service.

As the AAA study also stated, no silver bullet solution or technology exists that could address all requirements or solve all current issues. However, promising progress is being made in these areas. Enabling Users is gaining a greater understanding of practical needs in terms of Assurance vs. federation capabilities. Progress towards attribute release is also being made in the deployment of the CoCo. Finally, coverage is improving, with the number of IdPs in eduGAIN doubling in one year alone. As several federations are considering moving to an opt-out rather than opt-in model, this number is likely to quickly increase further.

Some of the problems and requirements analysed cannot be addressed in the short term. For example, the issue of LoA requires the development of a common understanding of LoA tailored to the higher education sector, possibly also including LoA for organisations (and their identity vetting processes), plus LoA for individual users with a different LoA to that of their organisations. Based on the Enabling Users experience, the organisational and business case aspects of delivering such a solution will be examined during future GÉANT projects.

Many research communities also requested non-web authentication. Moonshot is one potential solution to provide this, but is still in the early stages and not widely deployed, and also offers a unifying solution for Single Sign On that is too large for what some of the simpler use cases require. SAML ECP is an alternative method for supporting non-Web SSO and in some areas could lead to results faster. This option has been identified as requiring a deployment strategy within the eduGAIN environment.

As regards FIM, although it ultimately does reduce user management overhead and risks, it is a specialist field contained within a much wider systems administration and delivery skillset, so that the relevant know-how within research communities is often limited. Manpower dedicated to working on FIM within research projects is generally scarce, which made collaboration and planning sometimes difficult. Drawing up project plans with research communities is helpful in this respect, but the core purpose of the eResearch group is often a priority that overrides other concerns, and although FIM is important to research communities, their primary aim obviously remains the research itself. The ongoing availability of expertise and consultancy from the federation community on a national and pan-European basis is therefore critical to prevent wasting limited resources on reinventing the wheel or their being confused by the various options available.

Our experience is that the assistance, expertise and services that Enabling Users provided was generally very welcome, needed and appreciated by the research communities. Sufficient use cases have been identified for Enabling Users to continue work on collaborative pilots in future projects, complementary to the E-INFRA-7 call [\[E-INFRA-7\]](#). It is also recommended that the provision of basic eduGAIN consultancy on request to research communities should be continued, as it often results in positive and fast results given a relatively small effort. Consultancy also enables research communities to become familiar with the topic without too much upfront effort and investment being required on their part prior to their making work plans. Receiving basic consultancy from the Enabling Users team could therefore be the first step on the way to developing more advanced FIM use cases later on. In addition, the greater number of results generated by collaborative pilots increases the ability of the consultancy team to help more research communities more quickly.

Appendix A Collaboration with other GÉANT Tasks

A.1 Service Activity 5: eduGAIN

The eduGAIN task (SA5 T3) operates the basic eduGAIN infrastructure, including the eduGAIN Metadata Distribution Service (MDS). They host the eduGAIN knowledge base and will integrate the tools that Enabling Users develop into a coherent supporting services suite for eduGAIN. The eduGAIN team focus on increasing the number of federation members joining the service, while Enabling Users is more concerned with services and identity providers.

A.2 Service Activity 5: Federation-as-a-Service (FaaS)

The FaaS task's (SA5 T4) goal was to create a pilot infrastructure that allows an organisation to quickly deploy a SAML-based identity federation. While the primary target group of this prospective service are countries that do not yet operate a federation of their own, large research communities may also decide to make use of this service in order to operate their federation. In consideration of this, the Enabling Users task was also involved in the design of the pilot service and the FaaS team were also able to share information about what types of services were considered interesting for countries starting a federation.

A.3 Joint Research Activity 3 (JRA3): Attributes & Groups Task

The main work areas covered by this task are related to facilitating the exchange of group data, in particular to finalise the VOOT protocol, and the analysis of different attribute management models and group management systems. Both areas are relevant for research communities because, besides authentication, they most often also need (group-based) solutions for authorisation and access control.

A.4 **Network Activity 4 (NA4): User Identification & Liaison Task**

In view of its purpose, this task has good contacts with many research communities that have high networking requirements. An increasing number of these communities not only rely on good bandwidth but also need a solution for their FIM needs. Therefore, several research communities were referred to Enabling Users by the “User Identification & Liaison” task, and at times both tasks directly talked to research communities which had both bandwidth and AAI requirements.

A.5 **Service Activity 7 (SA7): Support to clouds**

The overall goal of this activity is to broker cloud services to the education and research community. One of their objectives is to make cloud services available that allow end users to subscribe or log in to these services in a federated way via eduGAIN. Therefore, the Enabling Users team provided its expertise where needed and helped SA7 in finding a solution for a consistent approach to the registration of cloud services.

References

- [AAA] AAA Study, Licia Florio (TERENA) et al, 2012
<http://www.terena.org/publications/files/2012-AAA-Study-report-final.pdf>
- [CERN] <http://www.cern.ch/>
- [CoCo] GÉANT Data Protection Code of Conduct
<http://www.geant.net/uri/dataprotection-code-of-conduct/v1>
- [DARIAH] <http://www.dariah.eu/>
- [E-INFRA-7] <http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/2141-einfra-7-2014.html>
- [ELIXIR] <http://www.elixir-europe.org/>
- [ESA] <http://www.esa.int/ESA>
- [FIM4R] “Federated Identity Management for Research Collaborations”, 2012, CERN-OPEN-2012-006, Broeder, Daan (MPI) ; Jones, Bob (CERN) ; Kelsey, David (STFC) ; Kershaw, Philip (STFC) ; Lüders, Stefan (CERN) ; Lyall, Andrew (EBI) ; Nyrönen, Tommi (CSC) ; Wartel, Romain (CERN) ; Weyer, Heinz J (PSI, Villigen)
<http://cds.cern.ch/record/1442597/>
- [GÉANT] GÉANT, pan-European research and education network
<http://www.geant.net/>
- [GN3plus] “Multi-Gigabit European Research and Education Network and Associated Services (GN3plus)”, DANTE (Matthew Scott, Niels Hersoug), 2012
- [GN3PLUS13-642-23] <https://wiki.edugain.org/index.php?action=remote&title=-&mod=SecureFileStore&rf=getFile&f=/a/a1/Options-for-Joining-eduGAIN.pdf>
- [isFederatedCheck] <https://wiki.edugain.org/isFederatedCheck>
- [RDA-FIM] <https://rd-alliance.org/groups/federated-identity-management.html>
- [REMS] Resource Entitlement Management System (REMS)
<http://rems.csc.fi/>
- [Policy] eduGAIN Policy
<http://www.geant.net/service/edugain/resources/Pages/home.aspx>
- [Wiki_eduGAIN] <http://wiki.edugain.org/>

Glossary

AA	Attribute Authority
AAI	Authentication and Authorisation Infrastructure
eduGAIN	educational Global Authentication Infrastructure
CLARIN	Common Language Resources and Technology Infrastructure
CoCo	GÉANT Data Protection Code of Conduct
DAC	Data Access Committee
DARIAH	Digital Research Infrastructure for the Arts and Humanities
EBI	European Bioinformatics Institute
EC	European Commission
EGA	European Genome-phenome Archive
ESA	European Space Agency
EO	Earth Observation
ESFRI	European Strategy Forum on Research Infrastructures
FaaS	Federation as a Service
FIM	Federated Identity Management
FIM4R	Federated Identity Management for Research – a forum for AAI providers, e-Infrastructures and users
FIMig	Federated Identity Management Interest Group of the RDA
FP7	Seventh Framework Programme for Research and Technological Development
GN3	GÉANT 3 Project
GN3plus	GÉANT 3 Plus Project
IdM	Identity Management
IdP	Identity Provider
JRA	Joint Research Activity
LoA	Level of Assurance
MDS	Metadata Distribution Service
NA	Networking Activity
NREN	National Research and Education Network
PKI	Public Key Infrastructure
REFEDS	Research and Education Identity Federations
RDA	Research Data Alliance
REMS	Resource Entitlement Management System
SA	Service Activity
SA5	Service Activity 5 “Application Services”
SAML	Security Assertion Markup Language

SCI	Security for Collaborating Infrastructures
SSH	Social Science and Humanities.
SP	Service Provider
SSO	Single Sign-On
VC	Video Conference
VO	Virtual Organization
VOOT	Virtual Organization Orthogonal Technology