Implementation of PKI IDP Management Systems for Access to Resources of European R&E E-Infrastructures

[1]Bogatencov Peter, [2]Pocotilenco Valentin

[1]RENAM Association
Str. Academiei, 5, of 332, Chisinau, MD2028, Republic of Moldova
E-mail: bogatencov@renam.md,

[2]Technical University of Moldova
Stefan cel Mare, 168, Chisinau, MD2012, Republic of Moldova
E-mail: pvv@renam.md

ABSTRACT

Contemporary level of scientific and technical development is due to sharing relevant information and in this case it is very important to organize access to various informational systems with protected informational resources. Implementation of right instruments for interaction with informational systems for research and educational communities is a real necessity and will have essential contribution to increase capacity for knowledge access. Information systems development trends are reinforced by international projects with different destinations but with a common purpose: scientific and technical development and R&E society stimulation. Such projects are implemented as services and they are accessible to all interested community, but by realization of access rules and approached that are based on digital certificates, identity management, auto identification and authorization systems implementation. Many services and informational resources in the pan-European GÉANT network and connected Research and Educational networks require implementation of Public Keys Infrastructure and identity management technology.

Keywords: GEANT, IT services, R&E, PKI, authentication, interoperability, securing, access, resources

1. IMPORTANCE OF MODERN E-INFRASTRUCTURES

Research infrastructures (e-Infrastructures) play an increasing role in the advancement of knowledge and technology and their exploitation. For example, radiation sources, data bases in genomics and data collections in social science, observatories for environmental sciences, systems of imaging or clean rooms for the study and development of new materials or nano-electronics, are at the core of research and innovation processes.

By offering unique research services to users from different countries, including from the peripheral and outermost regions, by attracting young people to science and through networking of facilities, research infrastructures help structuring the scientific community and play therefore a key role in the construction of an efficient research and innovation environment [1,2]. Because of their ability to assemble a 'critical mass' of people and investment, they contribute to national, regional and European economic development. They are therefore at the core of the knowledge triangle of research, education and innovation [3,4]. Modern e-Infrastructures are the new research environment in which all researchers - whether working in the context

of their home institutions or in national or multinational scientific initiatives - have shared access to unique or distributed scientific facilities (including data, instruments, computing and communications), regardless of their type and location in the world. E-infrastructure provides remote access to scientific data and instruments located in top-level laboratories around the world, and enables worldwide collaboration among researchers who work on similar challenges and are willing to share resources.

The e-Infrastructure layers consist of (see figure 1):

- Communication Networks (the European Research & Education Network GÉANT, National Research & Education Networks-NRENs);
- Distributed Computing (GRID, High Performance Computing, Cloud computing, etc.),
- Middleware (the intermediate software between any local IT resource management system and the applications),
- Specialized applications and software systems,
- Scientific data (data management systems, data repositories, e-Libraries, etc.).

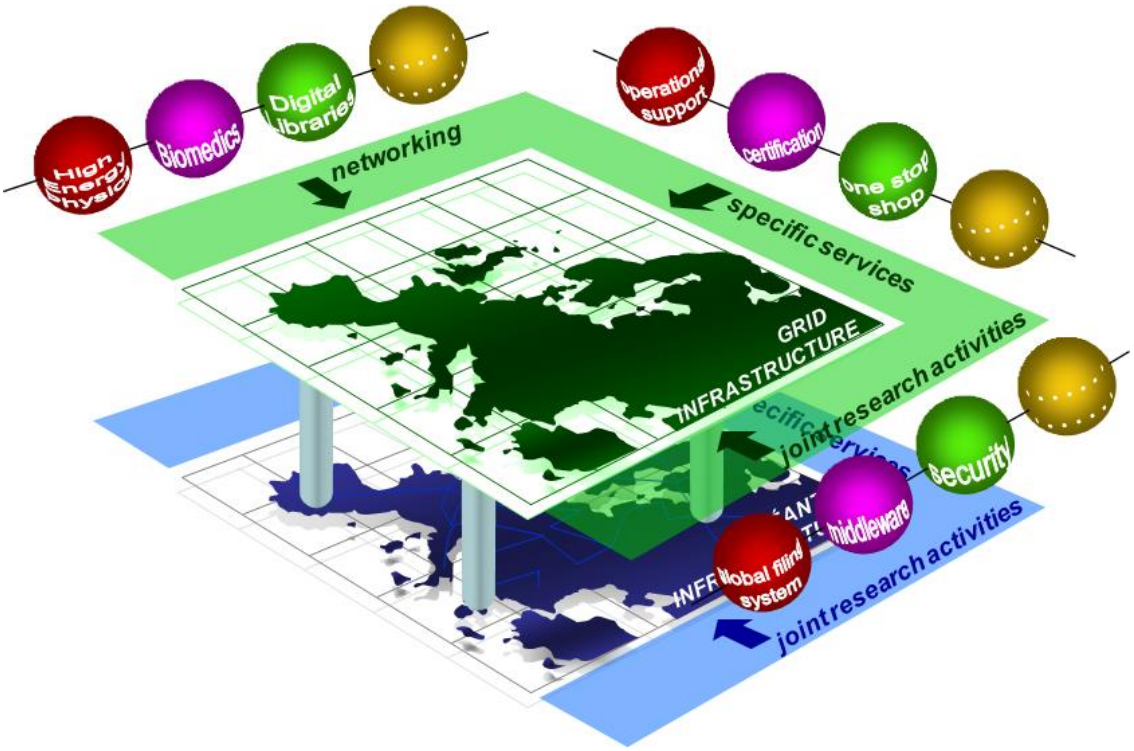

Figure 1. E-infrastructure - implementation blocks

e-Infrastructure stimulates the identification and creation of new scientific communities, uniting researchers who are working on in interrelated scientific areas, have needs to access to joint resources and reach new levels of collaboration. Researchers can gain access to jointly updating scientific data repositories and measurement instruments located around the world without the need to travel. The emergence of virtual organizations distributed throughout the world, helps researchers to share resources and to strengthen collaboration on common issues.

Widespread use of e-infrastructures represents also an effective answer to problems such as the digital divide and brain drain. This is demonstrated by the Large Hadron Collider at CERN, which is serving the

worldwide community of particle physicists [5]. To facilitate a rapid transition to e-Science, the European Commission and Member States have made significant investments in e-Infrastructures, including the pan-European research network GÉANT3, e-Science grids, data infrastructures and high performance computing. e-Infrastructures make a major contribution to the objectives of the i2010 strategy (Information Society Development) and the vision for the European Research Area (ERA), and have a key role in supporting the deployment of new research facilities [6,7].

Striving for world leadership in e-Science, establishing e-Infrastructures as a sustainable utility and exploiting them to promote innovation are the three vectors of a renewed European strategy to support the ground-breaking science of 2020 and beyond. This strategy calls for a major step forward in terms of the type and intensity of investment, better linking of research and innovation policies and coordination of national and Community strategies.

2. GEANT: E-INFRASTRUCTURE SERVICES INTEGRATOR

GEANT: e-Infrastructure Services Provider for the wide R&E Community

Basic, generic e-infrastructures include European networking infrastructure like the GEANT network, which connects the vast majority of Europe's research sector. It enabled more than 40 million researchers across Europe to interconnect to their counterparts worldwide. GÉANT is the pan-European data exchange network for the research and education community. It links national research and education networks (NRENs) across Europe, enabling faster collaboration on various international projects ranging from particle physics to life science and arts [8].

This network layer has been extended with a service layer built on top of it, through technologies like High Performance Computing (HPC), scientific Grid and cloud computing, which allow different kinds of resource aggregation and federation over the network layer. These developments have been largely academic, while the commercial sector builds generic solutions such as commercial Cloud computing accessible over commercial data networks.

These generic systems are available to all but not necessarily optimized for any specific use. Information systems development trends are reinforced by international projects with different destinations but with a common purpose: scientific and technical development and R&E society stimulation. Such projects are implemented as services and they are accessible to all interested community, but by realization of access rules and approached that are based on digital certificates, identity management, auto identification and authorization systems implementation.

Many services and informational resources in the pan-European GÉANT network require implementation PKI infrastructure and identity management technology [9]. Many services provided by GEANT are based on Federated Identity Management paradigm that requires implementation of distributed systems for users' authentication and trusted infrastructure of identity providers [10].

The GÉANT network is project driven and focused on understanding its users' requirements, offering services that meet their specific needs. In collaboration with connected NRENs, GÉANT is developing user-focused, multi-domain services aimed at delivering seamless network performance across borders and domains and to roll these out at national level to institutions, projects and researchers through the GÉANT Service Area. The list of currently deployed GEANT services presented on figure 2.

GEANT as main actor in R&E community development

The GÉANT project is focused on understanding its users' requirements and offering services that meet specific needs of research and educational communities. In collaboration with the NRENs, GÉANT is developing specific user-focused, federated and interrelated services aimed at delivering seamless network

performance across borders and domains and to roll these out at national level to institutions, projects and researchers through the GÉANT Service Area.

To apply User Access and Applications services to end users, network infrastructure should appear to be one seamless resource in which the many interconnected networks are invisible, but where access to confidential user-projected data remains controlled. In order to make this possible, GÉANT is building a set of interoperable systems that allow roaming access by verifying users' identities and rights, and granting access to resources as appropriate.

The Identity Provider (IdP) systems are implemented at campus level, for use by the institution's students and researchers. Were identity is verified using login and password combination issued by institution or, in most cases: digital certificates issued by Public Keys Infrastructures, developed and managed by NREN.

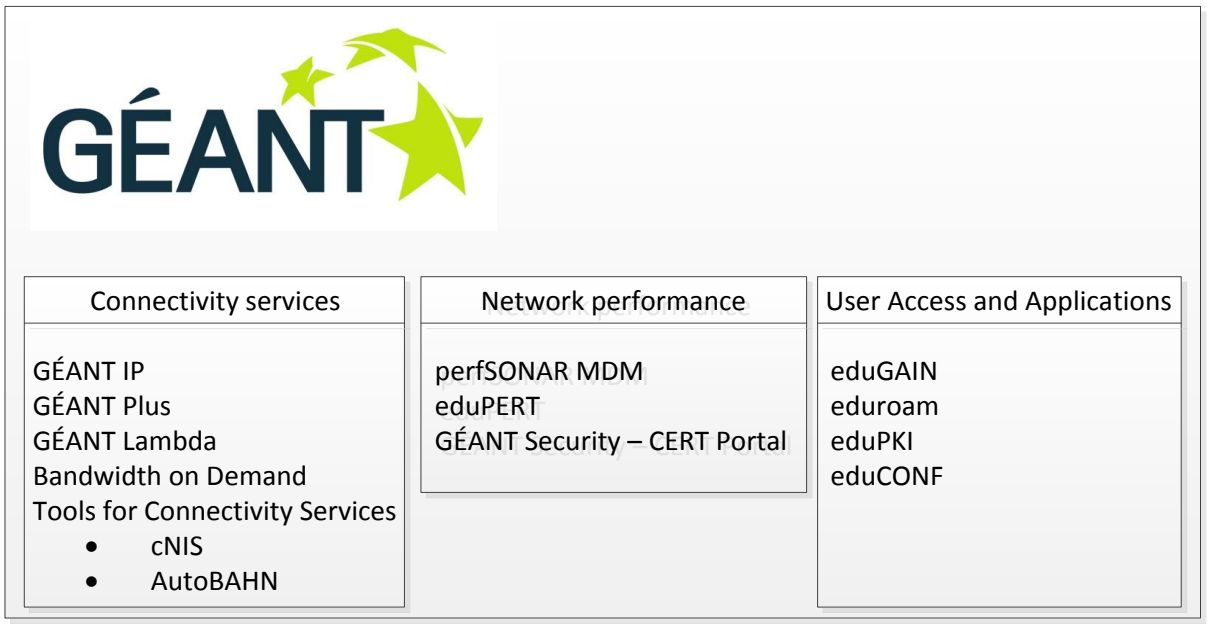

Figure 2. GEANT basic services

Current e- infrastructures and GEANT network as integrator of many e-infrastructure services face a number of challenges that threaten their ability to attract and retain users, make efficient use of resources, demonstrate value to funding communities, compete with commercial computing services and adopt sustainable governance models and funding structures.

The whole set of these issues can be generalize into two challenges, that of user satisfaction (including reliability, quality of service guarantees, usability and user retention) and that of sustainability (including understanding impact and costs, integration and standards, extension to new communities and governance models).

3. NREN AS PROVIDER OF E-INFRASTRUCTURE SERVICES AT NATIONAL LEVEL

As an example of typical NREN the Research and Educational Networking Association of Moldova (RENAM) operates the National networking infrastructure for Research and Educational institutions in Moldova. RENAM is a non-governmental, non-commercial and non-profit organization, established to promote and support the development of communication and information infrastructure for the scientific and educational community (especially higher and secondary education, research institutions, libraries and public collections, medical establishments), as well as to governmental organizations in Moldova.

Main activities of RENAM consist in constant development of communication and informational infrastructure and modern high-capacity communication media; creation of appropriate conditions for permanent networking infrastructure development for research and education by means of collaborated efforts of scientific and educational institutions; providing access to the national and foreign scientific databases and organizing access to scientific publications and educational informational content; permanent participation in extension of resources of the national e-Infrastructure; coordination and support of National Grid Initiative and Grid infrastructure development; providing access to the national, regional and European HPC resources. National R&E network now is capable to interconnect all research, educational, medical and cultural institutions from Moldova, and to provide them with Internet access, e-learning, e-science, Grid and high performance computing (www.grid.md) and other services [11].

In RENAM network was established and operating since 2009 Certification Authority as a basic element of National Public Keys Infrastructure for Research and Educational community, has begun deployment of basic instruments that are necessary for IT Services Management at national level and for interrelation with R&E service providers at European level [12, 13].

4. IDENTITY MANAGEMENT SYSTEMS

Identity management (IdM) refers to the policies, processes, and technologies that establish user identities and enforce rules about access to digital resources. In a campus setting, many information systems - such as e-mail, learning management systems, library databases, grid computing and HPC applications require users to authenticate themselves (typically with a username and password, digital certificate or using both authentication mechanisms). An authorization process then determines which systems (resources) an authenticated user is permitted to access [14].

Identity and access management ensures that the right people can access the right services. In the past, this was implemented system by system with duplicate identity data distributed across common infrastructure. If you are adding new service, you have to add the identity infrastructure to go with it. Now trying to manage the distributed security issues associated with these duplicate identity stores and you have similarly to duplicate your efforts and expenses.

The solution is to use the same identity information service for all your applications. This approach is exemplified in the fig. 1, if you integrate the data on the left and services on the right into the IdM infrastructure in the middle, then all the policies and procedures can be applied in that one spot in the center. This centralized and unified identity management allows [15]:

- Simplify and making more reliable authentication procedures by leveraging one IdM infrastructure over and over.
- Raising security level by consolidating your identity infrastructures from many to one and reducing the security procedures complexity from overwhelming to manageable.

Once the identity information about a person is consolidated, appropriate resources constituents can use tools to establish roles, grant access, add group membership as represented in the blue Enrich Identity and red Apply Policy boxes on the bottom of the diagram (see figure 3). The resource owners can define the specific interactions (called privileges) with that resource, such as purchasing materials or updating grades for a homework assignment.

Imagine setting up a standard “collaboration package” that includes group calendar, email list, wiki space, and so on, that campus individuals can request and then control who can have access to it, all without Help Desk intervention. In the past, these group memberships were not coordinated across services and had to be altered in each application when the members changed. Consolidating the groups and privileges allows

groups to change once in the IdM system and be "pushed out" to or accessed by the services in the collaboration package.

With the consolidation of identity information, the decision makers across e-infrastructures components can now also effect change much more quickly through interaction with the IdM system. This occurs because the IdM infrastructure becomes a bridge from the institutional processes and resource owners to the technology operations. It also enables the scaling of IT operations to meet the distributed needs and the mission of the institution; as the process and requirements evolve, the accompanying changes are made in just one place, the IdM system.

With a common e-infrastructure IdM system, rather than having separate credentials for each system, a user employing a single digital identity to access all resources to which the user is entitled. Federated identity management permits extending this approach above the single institution/e-infrastructure component level, creating a trusted authority for digital identities across multiple organizations or infrastructures.

In a federated system, participating institutions share identity attributes based on agreed-upon standards, facilitating authentication from other members of the federation and granting appropriate access to online resources. This approach streamlines access to digital assets while protecting restricted resources [16].

When a user affiliated with a member of a federation requests a protected resource from another member organization, the user is prompted for identifying information including his "home" organization. This request is passed to the home organization, which verifies the user's credentials and asserts to the requesting organization that the user has been authenticated. Federation members determine individually which attributes about users will be shared, such as name, title, or role.

Based on this information and their respective policies, member organizations then grant or deny access to particular resources. Users need only one set of authentication credentials - which could be a name and password or some other identity token - to access resources from other federation members. As a result, federated identity management separates access from the establishment of identity and authorization. Institutions no longer have to create and maintain large numbers of user credentials, instead managing identities only for their own users and accepting credentials from other federation members.

Attributes about users are verified by the home institution, which is most likely to have current, accurate information about the user, so there is no need to propagate status changes across multiple institutional identity systems. As student users graduate and assume new relationships with organizations, identity management systems in some cases can follow these changes and continue to provide appropriate access.

Despite the benefits of federated identity, the up-front costs to modify existing applications and systems can be an obstacle for some institutions. Federation membership might require different or more stringent identity protocols than an institution currently observes, and an institution might participate in multiple federations, each with unique requirements. Participating in a federation requires developing thorough institutional policies concerning access rights and compliance with the complex landscape of regulations. Although such policies and the work involved in writing them are beneficial, some institutions might not be ready to undertake such an effort.

The risks associated with unauthorized access to certain services are sufficiently high that provider organizations sometimes demand additional assurance from federation members. In these cases, a federation member might follow guidelines that set a higher bar for ensuring that credentialed users are legitimate. Over time, these kinds of measures are likely to deepen the trust in federated identity systems, but the process of getting there will require the complementary work of developing new protocols and revising expectations. In the meantime, a conservative approach to risk on the part of some institutions will slow adoption of federated identity practices. This contributes to a chicken-and-egg conundrum: lack of federation-ready institutions reduces the incentive to open applications to federated access, while a paucity of federation-ready applications makes the investment in a federated identity infrastructure less compelling to institutions.

As federated identity practices and systems mature, best practices and shared understanding will likely emerge, resulting in more consistent operational patterns for users and participating institutions. Research institutions, colleges and universities might not be the providers of "baseline" identities for employers and students. Rather, another entity would supply researchers, professors and students with credentials, and institutions might simply confirm that individuals are matriculated students or real employers, for instance, resulting in a distributed system of identity management that accommodates increased use of cloud-based services. If identity management indeed becomes user-centric rather than institution-centric, the issue of what entity serves as the originating and ultimate authority for digital identities will need to be resolved and agreed upon by participating organizations. Similarly, concerns about user privacy will need to be worked out to reassure users and ensure compliance with applicable regulations.

A growing number of research and educational resources and services are offered online, and users – research center, faculty, researchers, staff, students, alumni or others—increasingly expect access to these resources from various locations, including mobile devices. Identity management allows institutions, specialized resource owners to provide the access in a reliable, secure manner without a proliferation of credentials.

To the extent that federated identity allows institutions or even individual faculty to easily offer controlled access to research data or other resources, it has the potential to enable new levels of academic collaboration. Identity management can support institutional policies for extending access to valuable resources to certain groups of users, and the integration of identity management systems across academic, governmental, and commercial spheres further broadens the horizon for interdisciplinary, inter-institutional scholarship.

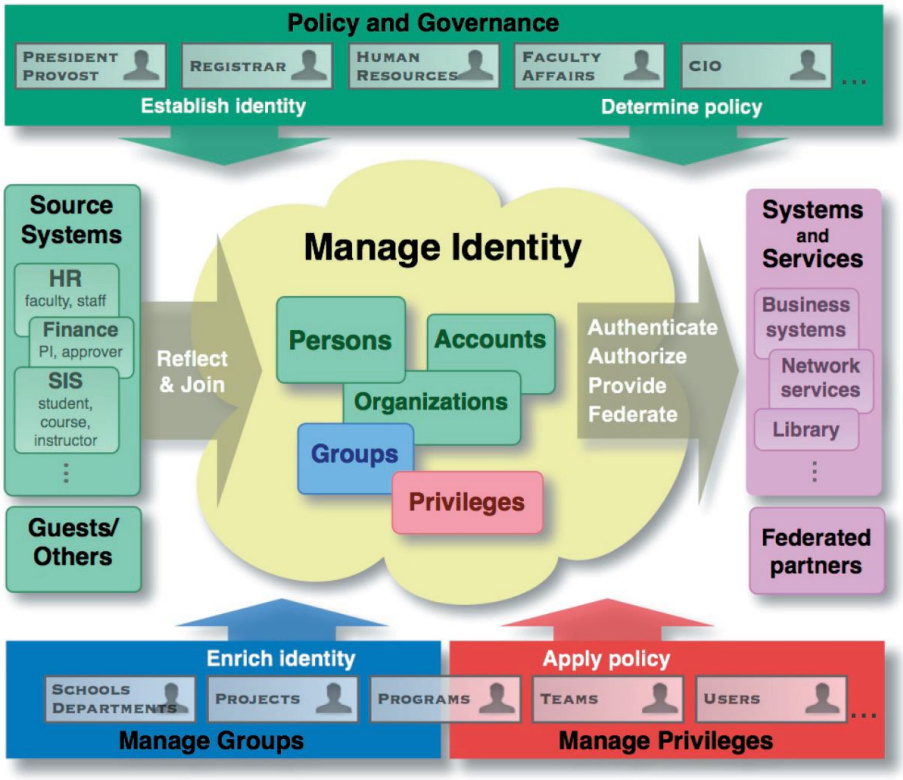

Figure 3. Model of the IdM system

5. EduGAIN - FEDERATED IDENTITY MANAGEMENT SERVICE IN GEANT

The eduGAIN service aims to establish a confederation of identity providers, enabling member organizations associated with different federations for securely exchange of information. There are many different federated systems in use across Europe, all of which are designed to control access to networks and applications, and ensure the secure movement of information within that network. It is currently necessary for organizations to join one another's federation in order to establish the relationship necessary to exchange information across these systems.

The existence of multiple federations makes it technically and administratively difficult for a user to access services offered by different institutions (e.g. outside of their own federation) and pass authorization log on procedure securely. When a user attempts to gain access to protected resources and services from other federations, they must first be successfully authenticated by their home Authentication and Authorization Infrastructure (AAI) and then to be authorized by the visited Service Provider. On figure 4 is presented the model of GEANT eduGAIN - federated IdM service implementation [16].

The eduGAIN service is intended to enable the trustworthy exchange of information related to identity, authentication and authorization between the GÉANT Partners' federations. The aim of eduGAIN is to enable different federations to interact. The information needed for locating entities in the different federations is centralized at a "Metadata Service (MDS)", where it can be dynamically queried and updated. By removing the logistical burden of connecting to foreign networks and dealing with unfamiliar systems, eduGAIN allows users to focus on their work, providing access to the resources they need.

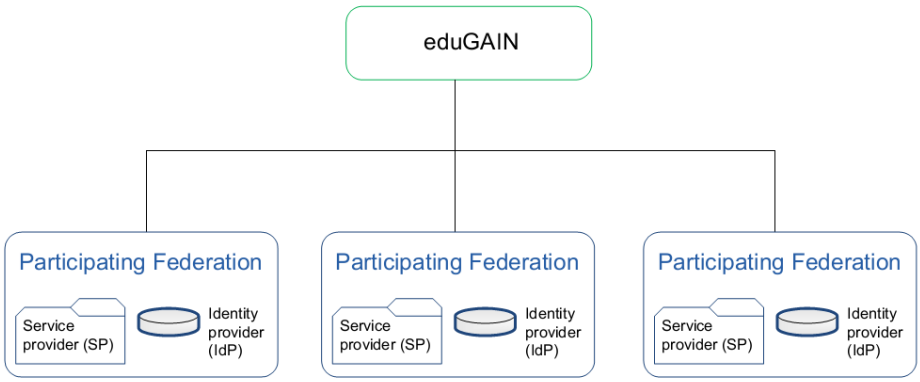

Figure 4. The eduGAIN operational model

Members of participating federations are able to communicate with each other and share metadata via a secure and trusted interaction. The sharing of metadata between federations enables end-users to benefit from a single sign on approach, which provides one-step login to all services provided by the federations.

6. STEPS TO JOINT GEANT EDUGAIN

First of all, it must exists at least one federation, which complies with minimum requirements, proposed by GEANT policy documents, regarding identity management service. Federation must ensure that containing only entities that agreed to join eduGAIN and that interested federations are in conformance with the eduGAIN Policy Framework. EduGAIN must have an appropriate mechanism to ensure that only entities, which have been checked and accepted by a eduGAIN Member Federation and which are in full conformance with the Policy Framework are exposed to eduGAIN.

In order to apply federation to eduGAIN infrastructure interested federation has to perform a few basic steps:

- First of all, for both types of members of federation (IdP and service provider - SP), the letter of intent is issued, which must be signed by a legitimate representative of organization and must express the will to enable inter-federation.
- For IdP must be received user consent.
- Local IdP must adapt its configuration to meet eduGAIN requirements:

  MUST be signed by a 2048 bit X.509 certificate

  MUST contain Publication Info element

  All entities MUST contain:

  - Registration Info element
  - Technical contact email address (role address)

  Not many MUSTs in general

  Entities SHOULD contain:

  - English name
  - (mdui:UIInfo->DisplayName)
  - English description
  - (mdui:UIInfo->Description)
  - Requested attributes for SPs (AttributeConsumingService)
  - Link to Metadata Registration and Practice Statement:
  - Describes processes how entities register with federation

  MDUI elements are useful for Discovery Service and Attribute Release

  Configure (missing) attributes recommended by eduGAIN

  - All of them are either static or can be composed of existing values
  - Other federations might have to instruct IdPs to adapt attribute release policy

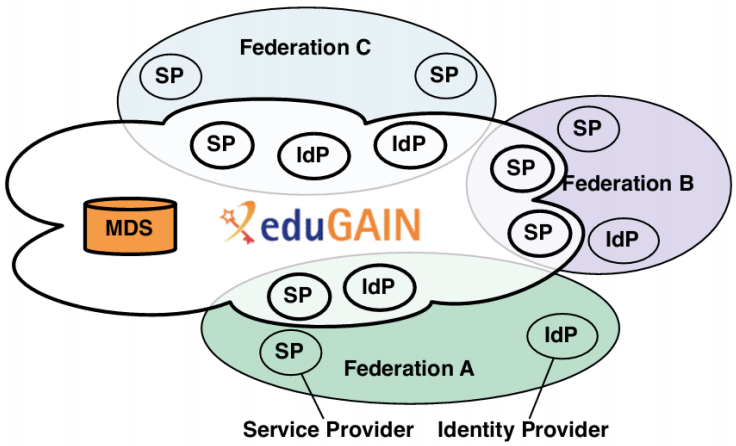

Figure 5. EduGAIN structure and members

- Next step is to adapt entries into Resource Registry, where inter-federated flows of metadata appear.
- Last step is inter-federation pass test. These tests apply last verification for metadata flow, if there are errors or inoperable metadata test return a detailed described cause of error. If all

requirements are met and no errors result from performed tests, IdP become able to communicate with most interfederated services provided.

EduGAIN metadata flow you can see on figure 6. Where: 1 - Federations publish upstream inter-federation metadata subsets; 2 - MDS aggregates all upstream metadata and republishes it; 3 - Federations process and republish eduGAIN metadata. Their inter-federation end entities consume it.

7. IMPLEMENTATION OF EDUGAIN COMPATIBLE IdM SYSTEM AT NATIONAL LEVEL

In order to provide access to GEANT resources at national level it is important to develop an IdM center operated by NREN, using NREN infrastructure and services [13]. Main goal is to establish a federation at national level, which will provide IdM services and will act as a gate to GEANT resources and services. At the national level, identity federation can act as unified national high-quality students, research and educational staff Human Resources data registry, where each participant will have personal right and attributes which will grant a specified level of access to national and international resources and services.

Main action in the process of federation developing is the writing process of internal policy, at national level. This policy must comply with national laws, have to offer the highest degree of interoperability and must comply with minimum inter-federation requirements, set by GEANT [17].

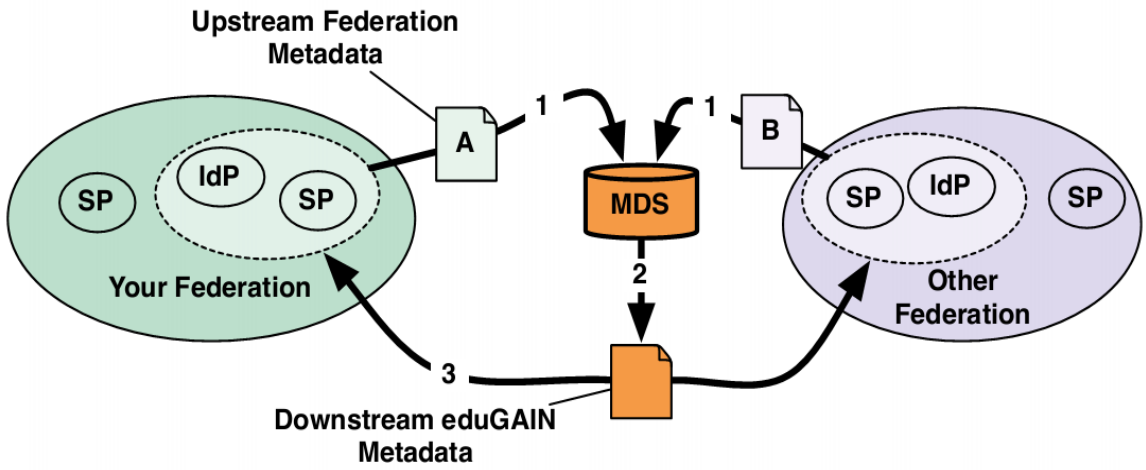

Figure 6. EduGAIN metadata flow.

Implementation of federative services at national level is long-term process, where the highest amount of time has to be dedicated to writing of polices and agreements and applying them to NREN institutions. All the services are dependent on IdP service, where identity and metadata exchange between federation or inter-federation members is the most important process for control access to networks and applications and ensure the secure movement of information within networks, informational systems and eInfrastructure resources in general.

REFERENCES

1. Work Program 2011. Capacities. Part I. Research infrastructures. http://cordis.europa.eu/fp7/ict/e-infrastructure/docs/wp2011.pdf.
2. Conclusions on the future of information and communication technologies research, innovation and infrastructures. 2982nd COMPETITIVENESS (Internal market, Industry and Research) Council meeting. Brussels, 3 December 2009,
3. http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/intm/111719.pdf.
4. Ljubljana Council 2008; Council Conclusions on "The Launch of the "Ljubljana Process" - towards full realization of ERA, http://ec.europa.eu/research/ era/partnership/process/ ljubljana_process_ en.htm
5. Green Paper; The European Research Area: New Perspectives, European Research Area, COM(2007) 161, http://ec.europa.eu/research/era/docs/en/understanding-era-european-commission-eur22840-161-2007-en.pdf.
6. ESFRI Working Group, http://ec.europa.eu/research/ infrastructures/index_en.cfm?pg=esfri-working-groups&section=e-infrastructures.
7. European Commission ICT Research in FP7, http://cordis.europa.eu/fp7/ict/e-infrastructure/home_en.html.
8. Europe's Information Society, www.ec.europa.eu/i, 2010.
9. Knowledge without Borders - GÉANT 2020 as the European Communications Commons. Report of the GÉANT Expert Group, October 2011. European Commission, Information Society and Media (http://cordis.europa.eu/fp7/ict/e-infrastructure/docs/geg-report.pdf).
10. Federating GN3 Services – GÉANT - http://www.geant.net/Media_Centre /Media_Library/Media Library/Federating GN3 Services posterWEB.pdf.
11. GEANT. Identity Federations - http://www.geant.net/Research/Multidomain _User_Application_ Research/Pages/IdentityFederations.aspx.
12. Andries A., Bogatencov P., Secrieru G., Sidorenco V. RENAM: National eInfrastructure for Research and Educational Areas (RENAM: eInfrastructura naţională ale sectoarelor de cercetare ştiinţifică şi învăţământ). IT-Moldova. Revista tehnologiilor informaţionale, N 1-2, Chişinau, 2008. P. 85-89.
13. Pocotilenco V., Sidorenco V., Altuhov A., Bogatencov P. Deploying Certification Authority – the Key Element in the Security Infrastructure. Proceeding of the 1st International workshop on Information Technologies and Security. ITSEC-2007, 15-16 October 2007, Chisinau, Free International University of Moldova, pp. 223-229.
14. Pocotilenco Valentin, Altuhov Alexei, Bogatencov Petru, Sidorenco Veaceslav. "Networking in Education and Research", Proceedings of RoEduNet International Conference, 8th Edition, Romania, Galati, December 3-4, 2009, pp. 44-46.
15. Windley Phillip J. Digital Identity. O'Reilly Media Inc., Printed in USA, 2005, p.234. ISBN 978-0-596-00878-9.
16. Identity and Access Management. Developed by the Internet2 Middleware Initiative. Web publication - http://www.internet2.edu/pubs/200703-IS-MW.pdf.
17. Solberg Andreas Akre, Hedberg Roland. GÉANT Federation Lab. Web publication, TNC2012, 21 - 24 May, Reykjavík, Iceland - https://tnc2012.terena.org/core/ presentation/26.
18. Brook Schofield, Introduction to Identity Federations. Web publication, EUROCamp2012, Building Federated Identity Policy - 15 October 2012, GN3 Symposium, Vienna, Austria - http://www.terena.org/activities/ eurocamp/oct12/slides/GN3-2012-Schofield-20121015.pdf.