Modern View on Access to Shared Services through Federated Identity Provider

[1]Pocotilenco Valentin, [2]Bogatencov Petru, [3]Sclifos Constantin

[1]Technical University of Moldova
168, Stefan cel Mare Bd., Chisinau, MD-2004, Republic of Moldova
Tel: 37367395240, e-mail: valentin.pocotilenco@adm.utm.md

[2]RENAM Association
Str. Academiei 5, Chisinau, MD-2028, Republic of Moldova
Tel: 37369151334, e-mail: bogatencov@renam.md

[3]Academy of Economic Studies of Moldova
61, Banulescu-Bodoni str., Chișinău, MD-2005, Republic of Moldova
Tel: 37367100878, e-mail: sclifcon@vle.ase.md

ABSTRACT

Modern 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. New instruments for improvement access to protected data resources are actively developing now and in the paper described possible approaches of their realization.

Keywords: federated, identity, services, management, access, provider, information, system, data

1. INTRODUCTION

Contemporary information needs and requirements are permanently growing. The wide set of information sources usually accessed that can be absolutely different from organization or destination point of view. As a result, the user has to use multiple credentials or data protection mechanisms to access them. To simplify the process of using information resources, many different identity management technologies were proposed. Identity management can be done at different levels, for example institutional, national, or international.

Different identity management technologies can be applied at each level. Institutional or national identity management typically employs locally developed implementations which usually comply with a part of identity management practices and fully satisfy local needs. At institutional or national level, SSO (Single Sign On) solutions are a simple way of sharing resources and services, but at international level more widely federated identity mechanisms are used.

2. IDENTITY FEDERATION AND SINGLE SIGN ON

Initially as a service access solution within a project (Figure 1), SSO technology has been expanded to facilitate access to geographically distributed services, evolving into national identity federations.

Figure 1. Microsoft SSO services

Example of SSO access mechanisms at the local level are the resources offered within an educational or research institution is depicted in Figure 2 [3].

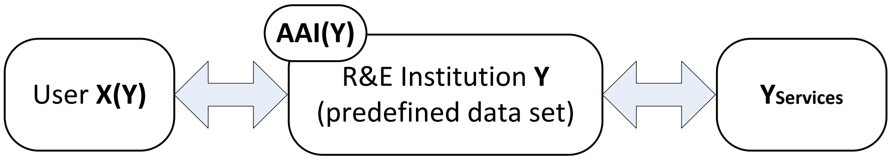

Figure 2. Institutional SSO implementation

Another example of a SSO mechanism is access to national e-resources by applying a single set of access data (Figure 3), as example – IDNO, or different datasets for each service.

Implementation of the models described earlier does not impose restrictions and the need to comply with the implemented AAI, the situation is completely different for the interconnection of national or international institutional resources.

To describe the above situation, we consider that there are two basic components need for federated mechanism functioning: IdM – identity management service; SP – service provider. We will consider that each institution can have at least one IdM and SP element (Figure 4.a). These institutions applying to common agreement will comply with a minimum set of data necessary for the effective operation of AAI. In this situation, each institution retains its data within its own IdM and authenticates/authorizes requests received from other members of the Federation Agreement. Such architecture is called mesh. Another situation can be considered when the IdM is done in a centralized form for shared services (Figure 4.b), the architecture being called Hub&Spoke. Such implementation increases the effectiveness of the authorization mechanism and simplifies the interconnection of resources at regional level.

Another advantage of Hub&Spoke topology is the reduction of costs and risks of maintenance of an IdM. In turn NREN can cooperate with similar organizations complying the AAI requirements for access to regional resources. The process of accession to the agreement for resource sharing is described as the process of establishing of Identity Federation. This process is widely supported within the pan-European GEANT network [1] through the eduGain inter-federation mechanism and disseminated through thematic meetings organized by GEANT Association[5].

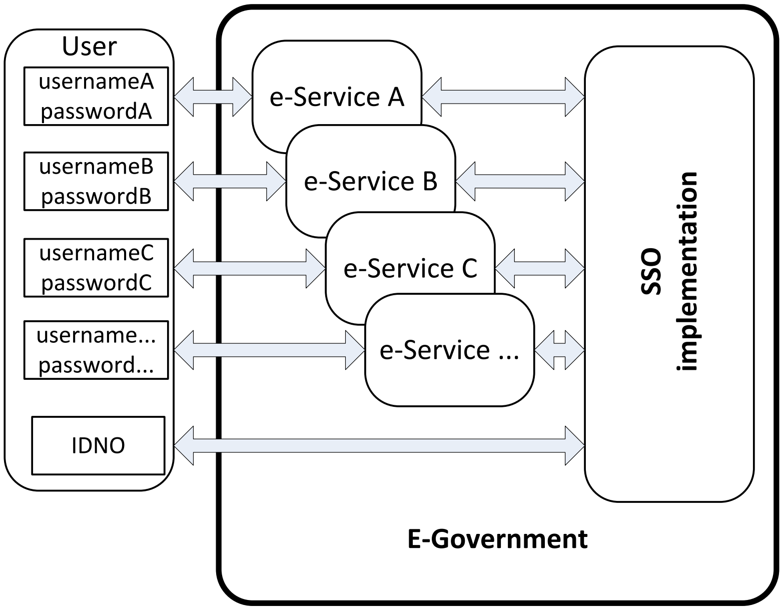

Figure 3. Example of national SSO mechanism

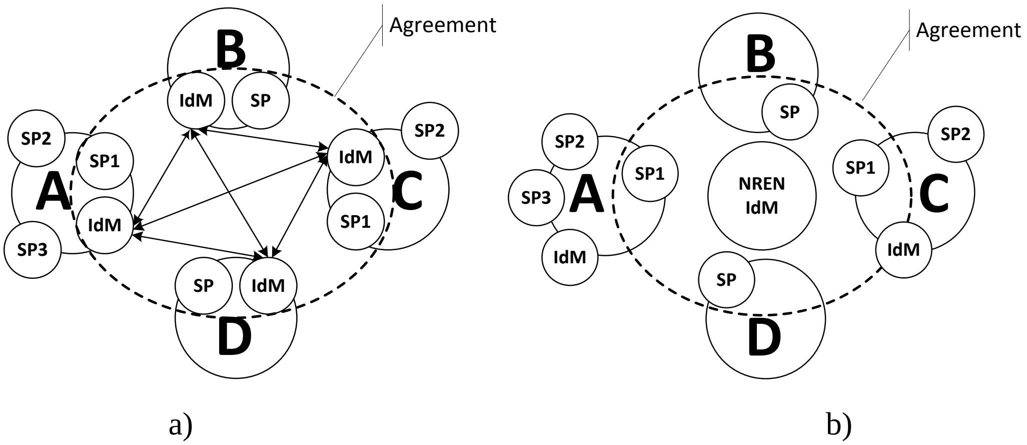

Figure 4. Federation topologies

It is necessary to take into account well-determined methods, requirements and principles, which must be followed by all its members, in order to implement a federated infrastructure for the purpose of resource sharing and access to services shared within eduGain [2]. For interoperation of federations within eduGain currently SAML2.0 is still used, because of large amount of included entities which use a wide range of software solutions based on it. Anyway contemporaneous solutions use more than one protocol for identity management systems, having SAML2.0 only for communication with eduGain, and within the organization network there are possibilities of using different protocols, based on specific data exchange needs (see Figure 5) [4].

An important aspect of security is the point of introducing sensitive data in the process of accessing the selected service. There are two ways to access federated services (as in the Figure 6) [6]. Depending on the SAML data middleware solutions shown in Figure 5, access to the requested service can be obtained by:

- SP initiated login – in this case, the user in institution B will first access the requested service (figure 6a) in institution A. Obviously in the institution A there is no information about the user, so located in the Federation SP will "ask" the IdM instance in institution B if the user is authorized to access the service. Authentication/authorization process will be initialized after redirecting to IdM. As a result, the user will be able to access the service.
- IdP initiated login – in this case, the user will log in to the IdM instance in institution B, thus the user will perform the authentication process. The next step is access to the service, if authentication/authorization process was succeed.

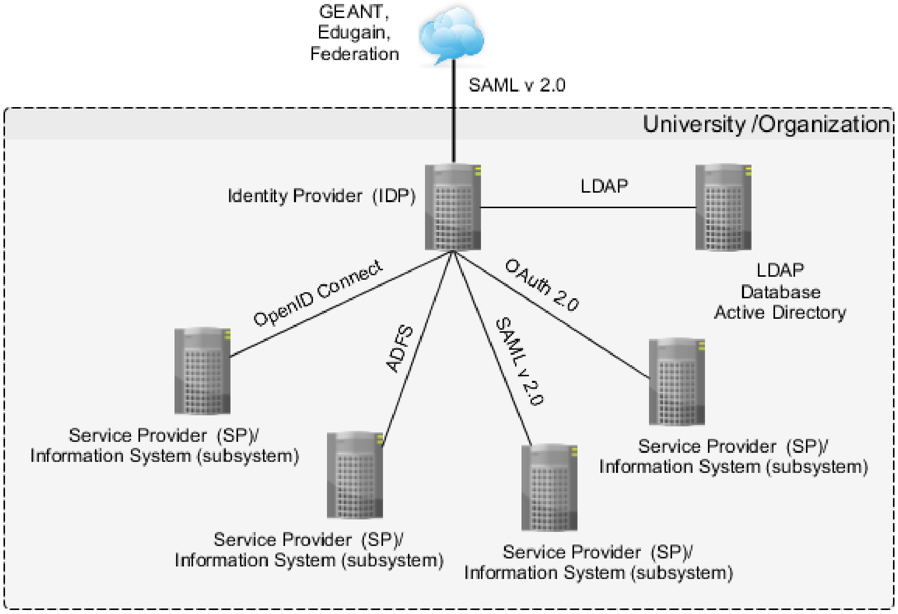

Figure 5. Example of protocols variety

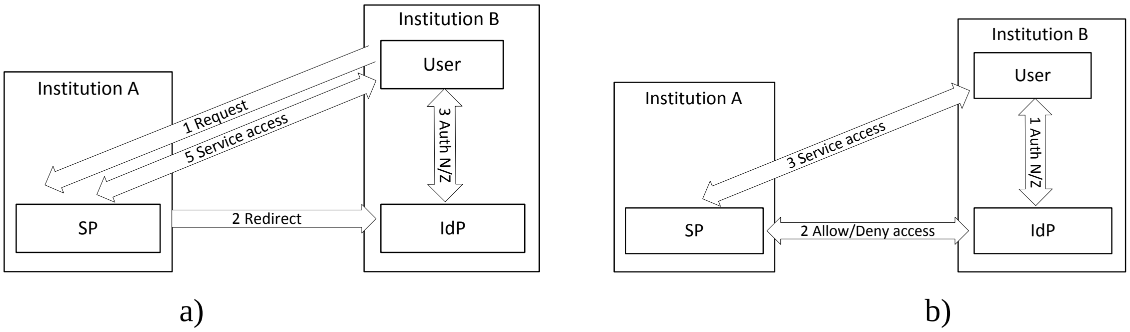

Figure 6. Access to federated services

4. IDENTITY FEDERATION

Access to interinstitutional resources without risk of personal data loss is an important moment in developing fruitful collaborations at national or international levels. In this sense, the operator of the National Research and Education Network RENAM launched identity federation that is named LEAF[7] and continues to improve it operation and used technologies in order to provide a modern service for Research and Educational community of Moldova. LEAF is operating the united internal IdM registered to eduGain, and offering access to three SPs for local purposes. In addition, in order to comply with tendences on identity management marketplace and to follow modern requirements, LEAF team continuously tests and deploying new operational solutions.

REFERENCES

1. www.geant.net, “Federating GN3 Services – Géant”

2. www.geant.net, “Identity Federations”

3. Bogatencov P., Pocotilenco V. Implementation of PKI IDP Management Systems for Access to Resources of European R&E E-Infrastructures. Proceedings of ITSEC-2012 International Conference on Information Technologies and Security, 15-16 October 2012, Chisinau: NCAA, 2013, pp. 227-237. ISBN 978-9975-4172-3

4. Bogatencov P., Pocotilenco V. Implementation of national IdP Management Systems for Access to Resources of European R&E E-Infrastructures. “Networking in Education and Research”, Proceedings of the 11th RoEduNet IEEE International Conference, Sinaia, Romania, January 17-19, 2013, pp. 96-100. ISSN-L 2068-1038.

5. https://tnc2012.terena.org/core/presentation/26, Andreas Åkre Solberg, Roland Hedberg. “GÉANT Federation”, TNC2012

6. http://docs.oasis-open.org, “SAMLV2.0 Technical Overview”

7. http://federations.renam.md, LEAF Federation description