AMRES
Serbian Academic Network

TERENA Networking Conference 2013 - Innovating Together

Title: Designing Identity Federation Policy, the right way

Authors: Marina Vermezović
Author Affiliations: AMRES, Bulevar Kralja Aleksandra 90, 11000 Belgrade, Serbia

Keywords: identity federation, policy, authentication and authorization infrastructure, interfederation, eduGAIN

Abstract

Historically, authentication based on IP addresses or shared accounts has been a common mechanism to access external resources. These approaches are simplistic and fail when staff, students and researchers are off-campus or need to access collaborative resources intended for an individual user.

Identity federation aims to solve this problem and allows campus authentication systems to integrate with a wide variety of services on campus, between campuses in a country and beyond. However, enabling identity federation demands a formalized policy that defines governance, roles, obligation and rights, procedures for membership application and cancelation and liabilities to ensure trust between federation participants. As identity federation provides infrastructure that supports transmission of personal information between different administrative domains, and even different countries, special care must be put into the defining policy document.

Approximately half of European countries have deployed an identity federation. Pioneers in this area are now reaching their 10 year anniversary. In this period significant knowledge and experience has been gathered through the operation of those identity federations, as well through joint work performed by communities such as REFEDS [refeds]. There are two indirect consequences to this:

1. Existing identity federation policies has evolved based on local needs; and
2. Due to emerging interfederation initiatives (e.g. eduGAIN [edugain]) there is a need for harmonization of those policies.

This eclectic structure makes it difficult to align policies and verify compatibility. On the other hand, there is still a significant number of countries which have yet to establish an identity federation (23 Partners in GÉANT3+ [gn3+]) and one of the barriers that they are facing is writing a policy.

The “Federation Policy Best Practice Approach” and “Federation Policy Mapping” analyses performed by REFEDS show that there are certain similarities between the existing identity federations’ policies. Those policies can be broken down into similar sections, but there are slight differences in content, naming and order. This leads to the conclusion that an identity federation template document that can be used by different countries should be created and can benefit both new federations and existing federations wanting to update their policy. Thus, the task of designing an Identity Federation Policy Template document (in further text: the template) was initiated by the eduGAIN activity.

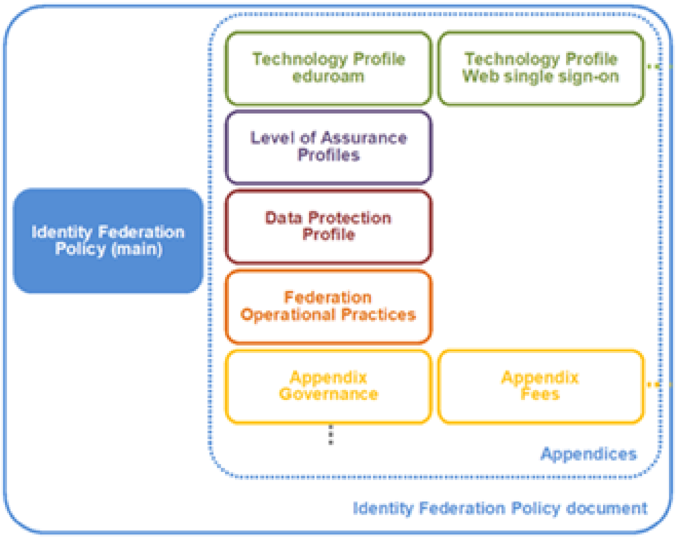

Technology Profile eduroam
Technology Profile Web single sign-on
Level of Assurance Profiles
Data Protection Profile
Federation Operational Practices
Appendix Governance
Appendix Fees
Appendices
Identity Federation Policy (main)
Identity Federation Policy document

Figure 1: Identity Federation Policy document suite

The template document is based on current best practices found in existing identity federation policy documents, both in terms of what to put, and what not to put in a policy document. Currently, there are several federation technologies which can make use of identity federation. For example, in many NRENs (national research and education networks) eduroam and Web single sign-on (WebSSO) are federated services which are widely deployed. Also, it is expected that new federation technologies that can use an identity federation will appear – such as Project Moonshot which is currently being developed and which should enable single sign-on for non-Web services. One of the important requirements when making the template document was to ensure that it allows for multiple technologies to be served while using the same policy structure. This further benefits federation by reducing the duplication of policy work. The structure of the policy document adopted by the template is similar to the concept of the SWAMID [swamid] identity federation policy and is presented in figure 1. This design of identity federation policy document suite allows for more flexible adding of new profiles at any point of operating an identity federation. The content and concept of the template document is based on the SWAMID identity federation policy and is released under the CC BY-SA 3.0 license.

Greatest challenges in designig the template document and methods used to meet those challenges were:

- Make the template independent of future technology changes or updates. To meet this challenge the concept of layering the structure of policy and operational documents is used. In this solution, only static and core issues are put into "main" policy document and all other issues are placed in appendices (e.g technology profiles).
- Avoid mistakes which are known problems in some of the existing identity federation policies (e.g. defining the federation will never enter interfederation agreements, defining exact list of types of organizations that can participate etc.). To meet this challenge, every section of the policy was carefully analyzed and the concept of not "over specifying" all issues is used, where detailed definitions are left to be placed in appendices or to be published on the federation web site.
- Write a general purpose document that can be easily reused. To meet this challenge special care was taken to write generic sections without merging the technology and trust components. However, certain issues are highly dependent on local circumstances (e.g. governance, liability) and for those the possible approaches are explained in detail.

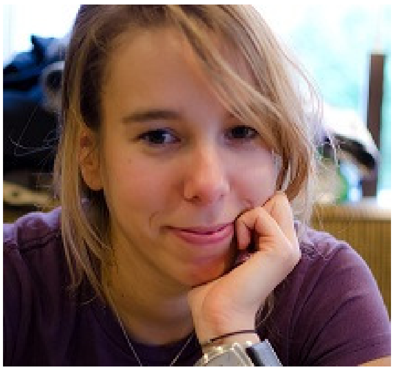
The template document was presented in the workshop organized in October 2012 and we got very positive feedback from participants representing 13 countries. So far, by our knowledge, there are at least three emerging federations and one existing which are actively working on their policy based on the template.

Acknowledgements

I would like to thank Mikael Linden, Peter Schober and Natalija Radošević, co-authors of the template document, who with their expertise and experience it this area helped to write and improve the document. Also, I would like to thank Nicole Harris, REFEDS coordinator, who gave a great input and Brook Schofield, leader of the eduGAIN task in GÉANT3, who made the initiative and delegated to me the task of designing the template document.

References

[edugain] eduGAIN web site: http://www.edugain.org/
[gn3+] GÉANT web site: http://www.geant.net/
[refeds] REFEDS web site: http://www.refeds.org
[swamid] SWAMID web site: http://www.swamid.se



Author Biography

Marina Vermezović studied at the Faculty of Electrical Engineering University of Belgrade. After graduating in 2006, she started working at University of Belgrade Computing Centre as a networking engineer and in 2012 when AMRES was formed as a legal body, she transferred to AMRES as the head of the department for user services. She has been involved in deploying AMRES eduroam and WebSSO federation, and has been participating in GÉANT eduGAIN and eduroam tasks.