SWITCH
Serving Swiss Universities

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

TERENA Networking Conference 2011 - Enabling Communities

Title: Trimming your AAI Federation fit for eduGAIN… technically

Author: Lukas Hämmerle (lukas.haemmerle@switch.ch)

Authors affiliation: SWITCH, Werdstrasse 2, P.O. Box , CH-8021 Zurich, Switzerland

Keywords: Federated identities, authentication and authorization infrastructure, eduGAIN, interfederation

Abstract

On 1. April 2011, a new era begins and borders will be crossed. Reason: The interfederation service "eduGAIN" [edugain] will start its production operation in GÉANT 3 [gn3]. Sharing web resources on a pan-European scale will become easier and more efficient thanks to the federated authentication provided by eduGAIN. Furthermore, users from participating organizations get access to more web resources and content.

By summer 2011, the major national federations are expected to already have signed the eduGAIN policy declaration. Thus, they become participant federations of the eduGAIN interfederation service. While this procedure legally is only a matter of signing a piece of paper, the job is not finished with the paper work. It also means making certain technical adaptations. These are non trivial.

EduGAIN is not a federation but a service for existing federations. It is up to every federation to become a participant federation of eduGAIN. Each Identity and Service Provider in a participant federation then decides whether to opt-in to eduGAIN or not. This is shown in Fig. 1. Due to technical complexities of such an interfederation setup, operators from participant federations should assist their member organizations in this process.

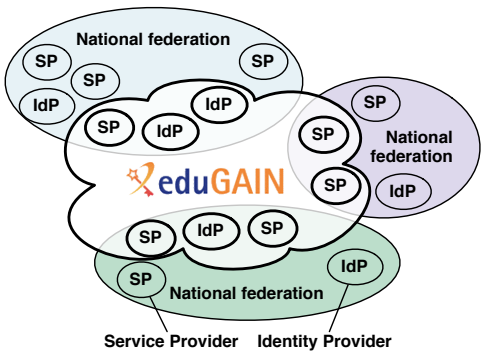

Figure 1: eduGAIN and local federations

In 2005 SWITCH started operating SWITCHaai [saai], the first production identity federation for higher education in Europe. Many more national federations followed. SAML 2 [saml2], the underlying technology of SWITCHaai, is nowadays the de facto standard for federated identity and access management in the academic world. Therefore, enabling services for interfederation could seem easy at first sight.

So far there weren't many attempts to expand existing federations across the national borders. Most Service and Identity Providers are members of only one federation, their national federation.

One regional attempt to establish interfederation is the Kalmar Union [ku]. It is a joint federation consisting of a subset of entities from five countries in Northern Europe.

EduGAIN's structure will be similar but will take interfederation to a new level. On one hand, the number of Service and Identity Providers will be considerably higher than in the Kalmar Union. On the other hand, eduGAIN will most likely also include entities from non-European federations in contrast to the Kalmar Union. This causes new challenges and problems to solve.

We present what adaptations were required for SWITCHaai in order to facilitate the step across national borders for our member organizations. Mostly technical topics will be covered. This includes the following areas:

Requirements
EduGAIN defines certain requirements that must be met before an organization can use the service. We will illustrate how we helped our member organizations meeting these requirements and how we shaped our federation processes to conform to these formal and technical requirements.

Metadata
Enabling a service for eduGAIN or another federation affects the generation, signing and distribution of federation metadata. We will show how we provide metadata for use in eduGAIN and how we process metadata for use in our local federation.

Attributes
Traditionally, each and every national federation uses a different set of user identity attributes. In eduGAIN, no attributes are mandatory to implement. There is also no attribute harmonization mandated. Nevertheless, it is recommended that the participating organizations release and accept certain attributes. We will demonstrate which steps were required as federation operator to facilitate the resolving of these attributes, how to assist Identity Provider administrators who have to manage attribute release policies and what means we provide for efficient attribute filtering on an organization level.

Deployment
Configuring an Identity or Service Provider for interfederation is non trivial. Various configuration files and access control rules must be adapted. The Identity Provider discovery problem becomes more difficult when a service can be accessed by users from hundreds of organizations instead of just a few dozens. We therefore will present means how to facilitate the transition from a service in the local federation to an interfederated service, accessible also from other federations through eduGAIN.

Summary
The presentation focuses on the changes and adaptations needed for becoming interfederation-ready from a federation operator's perspective. By the time of the TNC 2011, SWITCH will have completed the necessary steps to be ready for eduGAIN. The goal thus is to give the operators of other participant federations an overview of the problems and issues we faced while preparing our infrastructure for eduGAIN and for interfederating in general. We would like to show how to assist and support organizations that decide to opt-in for the eduGAIN interfederation service. On their own path towards interfederation, operators from other prospect participant federations can benefit from the experiences we made, they can re-use our approaches and they hopefully can prevent some obstacles we faced.

Acknowledgements

I would like to thank my colleague and project leader of AAI, Thomas Lenggenhager. Not only did he contribute many valuable inputs but he also helped improve this abstract considerably by proof-reading it several times on short notice. Also, I would like to thank Valter Nordh, leader of the eduGAIN task in GÉANT 3, who encouraged me to write and submit this abstract.

References

[edugain] eduGAIN web site: http://www.edugain.org/
[gn3] GÉANT web site: http://www.geant.net/
[ku] Kalmar Union federation: https://rnd.feide.no/kalmar_union/
[saai] SWITCHaai web site: http://www.switch.ch/aai
[saml2] SAML Oasis standard web site: http://saml.xml.org/

Author Biography

Lukas Haemmerle studied electrical engineering and information technology at the Swiss Institute of Technology (ETH Zurich). After graduating in 2004, he joined the middleware group at SWITCH as a software engineer. Lukas is primarily responsible for the development and the operation of the Shibboleth-based authentication and authorization infrastructure SWITCHaai, which SWITCH provides for the benefit of the higher education and research community in Switzerland.