An Identity Provider as a Service platform for the eduGAIN research and education community

Schmidt Michael
MNM Team
Leibniz Supercomputing Centre (LRZ)
Garching n. Munich, Germany
Michael.Schmidt@lrz.de

Ziegler Jule Anna
MNM Team
Leibniz Supercomputing Centre (LRZ)
Garching n. Munich, Germany
Jule.Ziegler@lrz.de

***Abstract*—A SAML Identity Provider (IdP) is the core entity required by organizations to connect to a national research and education (R&E) federation and, through it, to the global eduGAIN community. With growing networks, evolving technologies and higher security standards being introduced in (R&E), the task of creating and managing IdPs becomes more and more complex. The commonly used software solutions to deploy an IdP, e.g. Shibboleth and SimpleSAMLphp, both require hand-on experience on SAML and specific knowledge of the products. Furthermore, the global collaboration requires a growing set of configuration options to be implemented, for example standards and policies being introduced into the community or new identity attributes. The complexity has reached a point where it is very demanding for organizations to handle the technical challenges, leaving them unable to join the R&E community. To tackle this issues, an IdP deployment platform was designed to support especially small and medium sized organizations by creating an IdP and join a national identity federation.**

***Index Terms*—Federated Identity Management, Identity Provider, Research & Education, eduGAIN**

I. Introduction

Identity Management is an important topic in the infrastructure of todays organizations, because it controls how users interact with services. In order to allow users to access different independent services of an organization using a single account, the identity management is decoupled from each service and managed by an identity provider centrally. Identity federations are leveraging this concept and may then be spanned across organizational boundaries. In the research and education (R&E) area, this concept is applied to entire countries leading to national identity federations, which are called national research and education networks (NRENs). They provide a national authentication and authorization infrastructure to its members, which allows them to access many services. In order to connect multiple NRENs to each other, a so called inter-federation is needed. The european science project and association GÉANT [1] hosts the global inter-federation eduGAIN [2], which connects participants, 58 countries at the moment, world-wide. This enables researchers, staff and students of higher education organizations to collaborate on an international level, using their local user account.

However, the precondition to join the global eduGAIN community is an Identity Provider (IdP) using the Security Assertion Markup Language (SAML). Although there are existing software solutions, like Shibboleth and SimpleSAMLphp, it is very demanding to configure these tools correctly. Especially for small organizations with few IT personnel the installation and management an IdP often requires to much effort. To ease the deployment of IdPs and enable small and medium-sized institutes in particular to join R&E community, a platform to automatically spawn IdPs on server and cloud environments was designed. To maximize the effectiveness in the deployment of IdPs, it is very useful to automate the process as much as possible, thus reducing the chance of human-related misconfiguration errors, and, at the same time speeding up the whole process. First of all, an easy to use deployment Toolkit was developed, which is already available to the community as a GÉANT product [3]. Based on this, an entire software suite was created to embed the toolkit features in a platform to further simplify the creation and management of IdPs to a point where neither knowledge of the software tools nor the underlying infrastructure is needed. The overall goal is to provide an IdP-as-a-Service platform to the R&E community.

In this demo paper we briefly describe this work, focused on the implementation of an IdP platform for the R&E community that automates the deployment of an Shibboleth IdP. So far, the basic functionality for providing an IdP has been implemented.

II. Campus IdP Platform

The Campus IdP Platform aims to provide administrators a way to easily deploy and manage (cloud-based) IdPs for their home organizations. The IdP software installation might be on a local server as well as within a cloud environment. The overall goal of GÉANT providing a Campus IdP platform is to ease the daily life of its users by integrating in an unique system the management and archiving of metadata, installation and configuration tools to spawn IdP instances (on the Cloud), monitoring, in a scalable and convenient fashion.

The platform aims at providing functions for two user groups: Federation Operators (FedOps) and Home Organization Administrators (HomeAdmin). HomeAdmins should be supported in the creation and administration of an IdP. This includes production-ready configuration and integration into the corresponding federation. The FedOps use case is to

978-3-903176-15-7 © 2019 IFIP

manage an identity federation, which consists of multiple IdPs created by the platform. Today, the process of adding an IdP to a federation is done manually by contacting the FedOp directly. Most federations offer a website where HomeAdmins can upload the metadata of their IdP and request access to the federation. A federation specific approval process will be triggered that results in approving or denying an IdP. Once the IdP is approved, its users may access federated services.

The platform itself consists of one client and two server applications, as shown in the architectural overview diagram (figure 1). The web client, a Single-Page-Application build in React, provides an easy to use frontend to the user. It is configured as an eduGAIN service provider itself, allowing users to use federated login once an IdP is created. The client communicates via JSON with an API server, which creates, stores and manages the IdP configuration within its own database. Saving the configuration data in the API layer enables the reuse of configurations once they have been created. New or changed IdP requests are prepared and stored in a message queue, which automatically triggers the IdP factory server. The IdP factory server runs Ansible, using a template created out of the prepared configuration data, to spawn an IdP, either on an existing or newly created virtual machine. By using a microservice architecture, the platform consists of several independent components, which facilitates the exchange or addition of components. Complete IdP spawning time is of the order of few minutes, and involves the creation of the required resources on the cloud and virtualization platforms. Once created, a fully functional Identity Management System (IDM), consisting of Shibboleth, LDAP, Jetty and MySQL, is available to the user in the selected environment, which basically does not differ from a manually created one. The approach aims at automating the spawning process as much as possible, limiting the required input configuration parameters to a bare minimal set, but at the same time leaving the possibility to customize further the IdP configuration, if required.

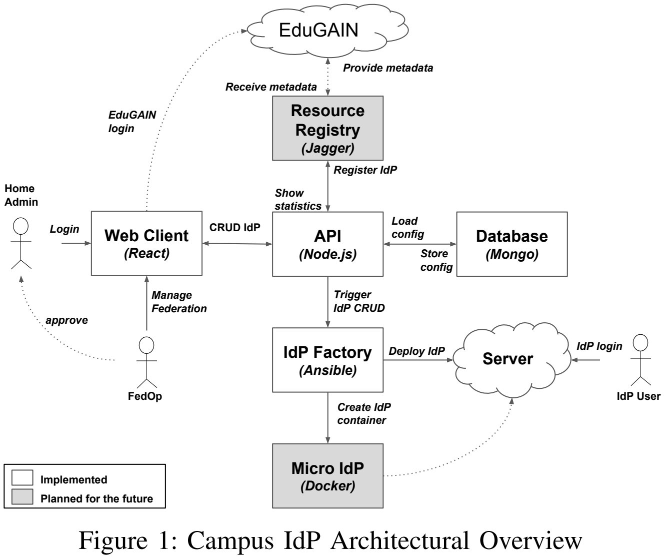

Figure 1: Campus IdP Architectural Overview

The entire system is designed highly modular by using the microservice architecture mentioned above. Another goal was to store the configuration information of an IdP in a technology independent format. Therefore, an abstract format based on the Resource Descrition Framework Schema (RDFS) [4] was created, which maps all the high level attributes of an IdP. This enables the potential use of stored configuration data in other services, which are using different data formats up to this day. The US federation Internet2 for example, has developed a similar solution to automatically configure and create Docker based IdPs. Using the schema, it would be easy to create an interface between these and similar systems or move data from one to another. This portability is a feature desired for an open research platform that most commercial cloud service providers in contrast lack today.

III. Conclusion

In this paper, the Campus IdP platform was presented. It is a first approach to provide an IdP-as-a-Service offering, which tries to ease the deployment of an IdP to enable especially small and medium sized organizations to join the global R&E community. Currently, the provision of an IdP is based on a manual installation and configuration of an existing software solution, which requires a lot of knowledge and effort. In comparison, the automated deployment with the Campus IdP platform offers the advantage of a simple and fast deployment, which can be used by an administrator even without special knowledge about identity management. The modular platform architecture ensures that software solutions can be adjusted easily, to support the needs of different federations. In future, this platform is planned to be extended to offer an extensive management view to control lifecycle aspects of an IdP or federation and include even more solutions provided by the R&E community. Additional software interfaces like the integration of a Resource Registry as well as a docker based deployment is already planned for the next project phase (Figure 1). By using the deployment platform, universities and research institutions are able to focus on their core research and teaching instead of IDM administration.

IV. Acknowledgment

The research leading to these results has received funding from the Europeans Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2). The authors want to thank all members of the Joint Research Activity 3 Task 1 and other persons involved in the design and implementation of Campus IdP.

References

[1] *GÉANT project homepage*, GÉANT Association. [Online]. Available: https://www.geant.org/Projects/GEANT_Project_GN4/Pages/Home.aspx (visited on 11/2018).

[2] *eduGAIN homepage*, GÉANT Association. [Online]. Available: https://edugain.org (visited on 11/2018).

[3] *GÉANT Ansible Toolkit*, GÉANT Association, Nov. 2018. [Online]. Available: https://github.com/GEANT/ansible-shibboleth.

[4] D. Brickley and R. Guha, *Rdf schema*, W3C. [Online]. Available: https://www.w3.org/TR/rdf-schema/ (visited on 11/2018).