Solutions to sharing institutional resources for collaborations

Presentor: Gerben Venekamp

Authors: Gerben Venekamp (SURFsara), Niels van Dijk (SURFnet), Harry Kodden (SURFsara), Paul van Dijk (SURFnet), Bas Zoetekauw (SURFnet)

Keywords: *authentication*, *authorisation*, *institutions*, *service development*, *non-web*, *federations*, *eduGAIN*

Introduction

Over the years, universities have developed many services to support local researchers. Whereas the focus for general applications seems to be shifting to the web, many research services---like storage, compute and scientific databases---remain solidly outside the web domain and are thereby hard to service by existing SAML-based identity management infrastructres.

With increased international collaboration, the need to share these resources in a scalably way with users from other organizations, both nationally and internationally, and both from academia as from comercial companies. To enable this, we need both proper authentication and a way to handle authorization. In addition, there is typically a need for the service provider to be able to delegate part of the authorization to principal investigators within the university.

This talk describes how SURF has developed a service, the Science Collaboration Zone (SCZ), based on the requirements of eleven communities and universities. SCZ was developed to enable institutions to easily yet securely manage and delegate access to both web based and non-web resources on their campuses. This paper reports what steps were taken to develop and deploy the service, both technically as well as in regard to policies. Finally, it also includes the results of testing the SCZ with these institutions and communities.

A three staged approach

While it is clear federated authentication, through eduGAIN, can be leveraged to solve the authentication part of this challenge in a scalable way, authentication alone is not enough to manage access to services. Membership and additional profile information needs to be recorded in a trusted way. Furthermore, enabling services to integrate federated authentication and authorization is often considered a challenge. In addition, SAML based authentication does not work for command line resources. This however is the major use case for many of the institutions. Finally, to allow services to be shared easily, enough trust must be established. Yet at the same time it is typically not the university IT department that has good knowledge of who needs access to resources and why. This trust needs to be delegated down into the institution both to the communities as well as to individual researchers.

Based on the requirements gathered from institutions and communities, SURF sought to create a service that would help institutions to more easily share their scientific campus services towards (international) collaborations. This service combines the ability to:

- Manage and delegate authorization to allow for easy sharing of services;
- Pragmatic, scalable support for non-web sso services;
- Reducing technical and policy support for providing and consuming eduGAIN servcies.

Manage and delegate authorization to allow for easy sharing of services

In line with the AARC Blueprint Architecture [1], SURF integrated three existing products: COmanage [2], SaToSa [3] and pyff [4] into a consistent service. By enhancing COmanage, SURF allows institutions and collaboration to self-manage memberships, roles and rights and services that are made available for the collaboration. Through integrating COmanage and SaToSa, the SCZ is able to deliver authentication and institutional attributes together with

collaboration roles and rights as part of the authentication flow for both SAML as well as OIDC enabled services. One of the major challenges was how to combine this new source of authorization into the existing back-end systems of the campus. We present a number of scenarios how to resolve this.

Pragmatic, scalable support for non-web sso services

The SCZ service offers a pragmatic approach to the non-web sso problem, with a two step process where a COmanage portal was enhanced to allow recording specific tokens. Next, non-web applications can use the information recorded to base their authentication and authorization decisions on. We showcase strategies for integrating back-end applications including distributed grid systems, iRODS and OpenStack.

Reducing technical and policy support for providing and consuming eduGAIN servcies

Connecting research services to eduGAIN requires a lot of expertise, which is often not available at institutions. To help researchers share their services the SCZ offers a proxied approach were services can be connected through SAML or OIDC. The proxy takes care of handling the interfederation requirements such as metadata handling on behalf of the connected services. At the same time the SCZ provides guidelines to services to help them engage with and live up to current best practice policies like R&S, CoCo and Sirtifi.

The presentation will also discuss how we used a standardised policy for the SCZ as a whole, to resolve common issues around attribute release toward services that are shared in the collaborations either locally or from eduGAIN.

Pilot results

:q

Together with the institutions and communities the SCZ was piloted. This presentation concludes with presenting the result of the pilots and the benefits as perceived by researchers, communities and institutions.

Presenter's bio

Gerben Venekamp has obtained his master degree in Artificial Intelligence at the University of Amsterdam. He then worked on authentication and authorization within the Grid community. Specifically, he worked on getting local accounts based on global Grid identities, which in turn was based on X.509.

After a detour in renewable energy and autonomous agents, Gerben returned to the field of AAI by joining SURFsara in 2015, where he works on developing a service for enabling non-web sso.

Session description

Creating intelligent complexity: collaboration

References

[1] https://aarc-project.eu/architecture/

[2] https://spaces.internet2.edu/display/COmanage/Home

[3] https://github.com/IdentityPython/SATOSA

[4] http://pyff.io/