Task 1 - Attributes and Authorisations

Introduction

These are the information pages of **GN4-1-JRA3-T1** also known as the research task on **Attributes and Authorisations in the Federated Identity Ecosystem**.

✓ If you have any questions or remarks: feel free to contact Maarten Kremers (Tasklead)

Objectives

The objectives of this research task are to:

- **Putting the user in control** by working on distributed and user controlled authorisation. Making collaboration and authorisation management platforms such as HEXAA and PERUN interoperate and contributing to the work on User-Managed Access (UMA).
- **Increasing usefulness of groups**, by introducing group awareness into appropriate cloud service middleware such as OpenStack.
- **Further improving group management**, by continuing work on VOOT specifications based on input from use-cases and extending additional group-aware applications with VOOT support.
- **Stimulate user-centricity for identity federations**, by studying implications, benefits and costs of moving from an organization-centric identity management model to a (more) user-centric identity federation model such as provided by eduID developments in various federations.

Results

✓ The results and dissemination of this task

Distributed Authorisation

- Paper Collaboration between SAML Federations and OpenStack Clouds at http://arxiv.org (Abstract / Paper)
- Shibboleth authentication plugin for Openstack at https://github.com (code)

EduKEEP

- Presentation EduKEEP concept at the Internet2 TechExchange 2015. (Abstract / Slides)

People

The following people are part of this task

Affiliation	Name
SURFnet	Maarten Kremers (Tasklead)
CESNET	Michal Procházka
CESNET	Slávek Licehammer
GARR	Lalla Mantovani

GARR	Marco Malavolti
GARR	Andrea Biancini
NIIF	Kristóf Bajnok
NIIF /MTA-SZTAKI	Mihály Héder
NORDUnet / Umeå Uni	Roland Hedberg
NORDUnet / Umeå Uni	Rebecka Gulliksson
RedIRIS / Uni Murcia	Alejandro Perez Mendez
SWITCH	Christoph Graf
SWITCH	Rolf Brugger

Workitem

In order to reach our goals the objectives are divided in the the following Work Items

- Distributed Authorisation
- User-Managed Access Controlled Attribute Service
- Towards User-Centric Identity Management Model: EduKEEP

Distributed Authorisation

People

- Héder Mihály (lead)
- Kristóf Bajnok
- Michal Procházka
- Slávek Licehammer
- Alejandro Perez Mendez
- Marco Malavolti
- Andrea Biancini

Goal / Workplan

Putting the user in control via distributed and user controlled authorisation.

- exploiting results from the HEXAA open call project and other initiatives around disturbed AuthZ.
- Standardisation / interoperability of these systems
- Delegation model of accessing the AA information

Increasing usefulness of groups

- Groups awareness for OpenStack

Improve Group Management

- Extend group-aware applications with VOOT
- Produce or stimulate implementations of VOOT

Documents / Links

Distributed Authorisation Documents on Google Drive (Access on request)

User-Managed Access Controlled Attribute Service

People

- Roland Hedberg (lead)
- Rebecka Gulliksson

Goal / Workplan

A Proof-of-Concep for a UMA controlled attribute service.

An application which would ultimately allows an user to control access to all her attributes in one place and can be used by SAML2 IdPs and AAs or OpenID Connect OPs as their attribute sources. The way the application is to be build, it will be build independent of the implementation of the IdP and AA. They all should be able to use the same attribute service. All that is need is a common API.

Documents / Links

- https://kantarainitiative.org/confluence/display/uma/Home
- https://wiki.larpp.internet2.edu/confluence/display/LARPP/Basic+architecture+discussion

Towards an User-Centric Identity Management Model: EduKEEP

People

- Maarten Kremers (lead)
- Andrea Biancini
- Marco Malavolti
- Christoph Graf
- Rolf Brugger

Goal / Workplan

Most, if not all, identity federations participating in eduGAIN manage users in an organization-centric fashion, which has several implications, like users changing organizations get issued new identities, even though they are linked to the very same person. An other case is that if no suitable primary affiliation exists (students leaving university or research collaboration with industry partners), there is no straight-forward way to get issued a valid identity at all.
In both cases, access to resources is lost, regardless of whether access rights were based on affiliation or on an individual basis.

Moving from an organization-centric identity management model to a user-centric model would do the trick, based on long-lived identity provider where the user is in control. Existing identity providers will become attribute providers serving information about the relationship with the individual. The long-lived identity provider will release basic information, combined with the additional attributes from the attribute providers.

Documents / Links

- EduKEEP Documents on Google Drive (Access on request)
- EduKEEP Presentation at Internet2 TechExchange 2015 (abstract, presentation)
- EduKEEP Summary of work (pdf)

Question? / Remarks?

Please contact Maarten Kremers