11-04-2016

Deliverable D15.1
Report on the Achievements of JRA3 Trust and Identity Research Task 1 Attributes and Authorisations and Recommendations on Future Work

Deliverable D15.1

Contractual Date:	30-04-2016
Actual Date:	11-04-2016
Grant Agreement No.:	691567
Work Package/Activity:	15/JRA3
Task Item:	Task 1
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	SURFnet
Document Code:	GN4-1-16-2854E
Authors:	R. Poortinga-van Wijnen (SURFnet)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Abstract
This deliverable reports on the achievements of Joint Research Activity 3 Trust and Identity Research, Task 1 Attributes and Authorisations during GN4-1 in the areas of multiple attribute authorities, distributed authorisation and group management, and a more centralised user-centric approach for identity federations. It also makes recommendations on future work.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This deliverable reports on the achievements of Joint Research Activity 3 Trust and Identity Research, Task 1 Attributes and Authorisations (JRA3 T1) during GN4-1, and makes recommendations on future work.

Within the realm of Trust and Identity, federated access management (FAM) is recognised as the standard approach to provide access to applications, both in the research and education (R&E) community and in the commercial world. However, the greater demand for FAM also brings new requirements for dynamic management, greater security, groups, best practices, support for all varieties of applications and so on. To focus the research in this Task, the following objectives were set:aai

- Increase the usefulness of groups.
- Put the user in control.
- Stimulate user-centricity for identity federations.

The work items on distributed authorisation and group management improved the interoperability between the various group management solutions (such as HEXAA, Grouper, and Perun) and demonstrated the feasibility of linking these solutions to an OpenStack environment simultaneously via eduGAIN. Solutions were provided for Security Assertion Markup Language (SAML) as well as for Moonshot, the former allowing users to log in to the (web-based) dashboard of OpenStack, the latter providing command line authentication and access. Recommendations for future work, for both solutions, include a standard method for user-deprovisioning and standardisation of a scoped entitlement attribute.

The eduKEEP work item looked at user-centricity for identity federations. Several federations already have – or are looking into – a more centralised form of federation setup, typically by employing a form of “eduID”, allowing a single identifier to be used to which other identities and attributes can be linked. The common factor in the different setups is the three distinct phases in the login process: authentication, identity enrichment, and service access. The Task’s work has shown that having a long-lived identity is a solid foundation on which to go forward with a (more) user-centric identity management federation model.

Initial work on a new, user-managed access standard has been shown to deliver significant benefits. It is recommended that the work be resumed in the next phase of the GÉANT project.

JRA3 T1 has carried out several high-profile dissemination activities during GN4-1. It is recommended that the level of activity be maintained, particularly with regard to eduKEEP, to elicit input as to its future development.

1 Introduction

Federated Access Management (FAM) and identity federations have, over the past decade, proved to be a great enabler of collaboration across institutional borders by facilitating the sharing of services and resources between different users of various institutions in a secure and (mostly) user-friendly manner. To provide a context for the research carried out within GN4-1 Joint Research Activity 3 Trust and Identity Research, Task 1 Attributes and Authorisations (JRA3 T1), this section gives an introduction to federations and their role in research and collaboration, thereby highlighting some issues as well as placing the research topics described in the following sections into perspective. The section also outlines the initial objectives of JRA3 T1.

1.1 Federation Basics

In the archetypical setup of FAM, Identity Providers (IdPs) vouch for the identity of their users, while Service Providers (SPs) accept these assurances and allow usage of the service they provide based on those assurances, as shown in Figure 1.1.

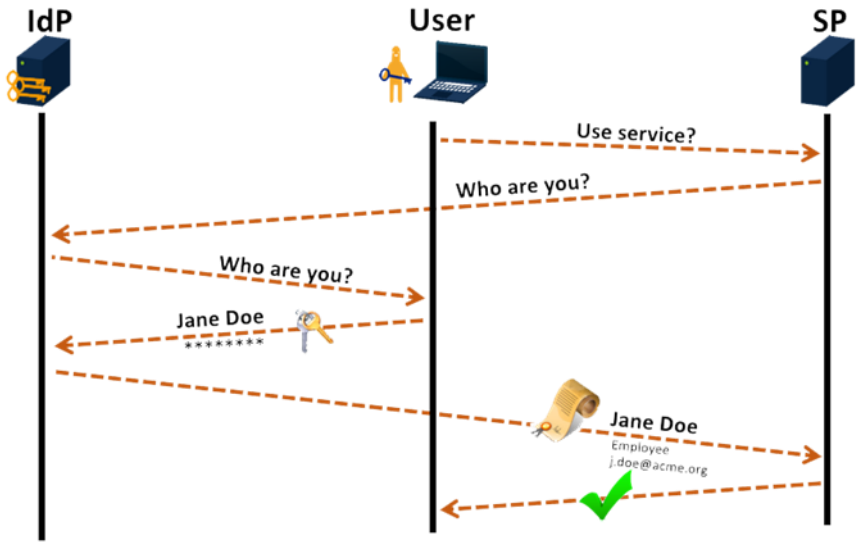

Figure 1.1: User logging in to a service after authentication by his IdP

An essential prerequisite for this setup is trust between SPs and IdPs, which is provided by an underlying set of – usually standardised – contracts. A collection of such contracted IdPs and SPs is called an identity federation and it is another prerequisite for the setup to work. The benefits it provides to all entities involved include:

- Users log in at their IdP, rather than at the service itself, after which the IdP provides an assertion to the SP that the user is indeed valid; the assertion is usually accompanied by some additional information about that user (called attributes). This also means that users only need to remember credentials for their institutional account for all the services they can access via the federation, instead of one account per service. Additionally, this lowers the temptation – or indeed the need – for users to reuse credentials across different services.
- For Identity Providers it is easier to procure and/or outsource services to external providers in an easy and standardised way, while also knowing that access to those services is easier for their users.
- Service Providers can more easily reach groups of users via IdPs by joining a federation, while at the same time not having the burden of user support with respect to account management (the ubiquitous “I've forgotten my password . . .” issue, for example).

The role of the federation operator (typically a national research and education network (NREN) in R&E federations) is to maintain the technical and trust fabric. This entails keeping track of contracts and policies, and providing the metadata for the federation (Figure 1.2), which can be seen as the telephone directory of the federation that allows IdPs and SPs to connect to each other and exchange the necessary information to make the setup work.

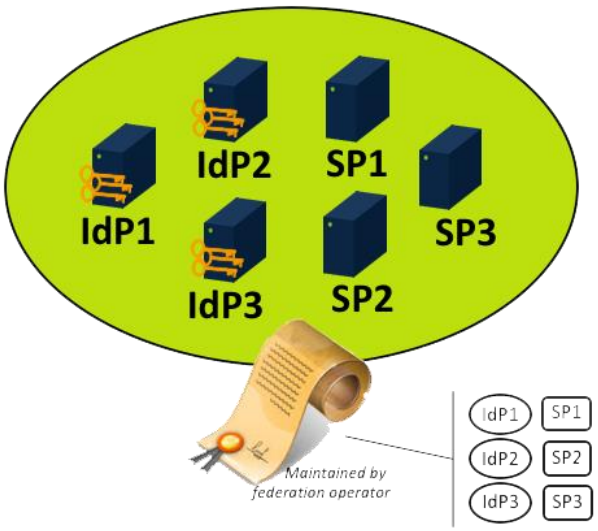

Figure 1.2: Identity federation with metadata describing the entities

Identity federations have seen a sharp uptake in the past decade, especially in the field of research and education. The largest initial uptake based on the typical federation setup and scenario

described above was due to “campus-centric” scenarios, that is, users from an IdP accessing specific services, typically procured by their institution, with the Service Provider offering one specific service instance per IdP.

1.2 Role and Challenges of Federations in Research and Collaboration

1.2.1 Access Rights to Services

The services that researchers use can be quite specialised and specific to their particular field of research, apart from a number of generic services such as wikis, content management systems (CMSs), etc. This means that only a small subset of all the users from any research IdP need (or should get) access to a specific service. Most federations are set up such that the IdP is responsible for limiting access to different services to different groups. Alternatively, some services allow access to be granted by adding specific attributes to the assertion sent to the service when the user authenticates. In other words, after checking that the user is authenticated by the IdP, the service will also check for the presence and proper value of an attribute. Typically the eduPersonEntitlement attribute is used for this purpose, with the service checking it for a specific value (e.g. `urn:mace:exampleIdP.org:demoservice:demo-admin`).

Both approaches mean that administrators of the IdP in question have to take special action to ensure that only the “right” users are allowed through to that service or to ensure that the proper entitlements are set for those users. While in itself this may not be too difficult or too much work, the number of faculties and specialised fields of research (with accompanying number of services) within an average university and the typical “distance” between those groups and the – usually centralised – administrator of an IdP make this approach cumbersome and labour intensive.

1.2.2 Single/Multiple Tenancy

The biggest use-case for identity federations in research is collaboration, with which, however, the typical campus-centric approach does not necessarily align neatly. Especially if a Service Provider offers a single service instance per Identity Provider (often referred to as “single tenant”), collaboration using that service is impossible if the users who want to collaborate come from different IdPs (since due to the single-tenant nature, they cannot “see” each other in that service).

1.2.3 Group Management

The challenges of using federations for collaboration in research and education do not stop there. If groups of users from multiple IdPs need to work together using a single service, then there also needs to be some way in which these groups can be assigned different sections or work spaces in that service. The straightforward approach for achieving that goal would be to create some form of authorisation and group management functionality within the service itself, allowing groups of users

and their different roles within that group (e.g. administrator, editor, user) to be managed; and indeed a lot of services provide just such functionality in one form or another. This approach works very well for the simplest collaborations.

1.2.4 Group Management across Services

However, most collaborations do not use a single service. Instead, they use a number of services to work together. A typical example would be an email list server for exchanging mails, a wiki for working together on draft documents and a content management system for the "official" publications by that group. If all these services use the approach described above, then the groups have to be recreated at every service the collaboration uses, which leads to a considerable overhead for the members tasked with this. In addition, it will most likely lead to mistakes and questions about which group definitions are the "right" ones. Clearly, the straightforward approach of group and authorisation management – (re)creating them in the different services – does not work well in these cases.

1.3 Attributes and Authorisations Task Objectives

The objectives of the Attributes and Authorisation Task (T1) within JRA3 were to research options for improving attribute-, group- and access-management solutions to address the challenges described in the previous sections. Specifically, the objectives in the project plan were defined as:

- **Further improve group management**, by continuing work on Virtual Organisation Orthogonal Technology (VOOT) specifications based on input from use-cases and extending additional group-aware applications with VOOT support.
- **Increase usefulness of groups**, by introducing group awareness into appropriate cloud service middleware such as OpenStack.
- **Put the user in control** by working on distributed and user-controlled authorisation. Make collaboration and authorisation management platforms such as HEXAA and Perun interoperate and contribute to the work on user-managed access (UMA).
- **Stimulate user-centricity for identity federations**, by studying the implications, benefits and costs of moving from an organisation-centric identity management model to a (more) user-centric identity federation model such as provided by eduID developments in various federations.

The first three objectives were tackled by the Distributed Authorisation and Group Management work item in the Task. The last objective was handled by the eduKEEP work item. The achievements of these work items are outlined in the next section.

2 Achievements of the Attributes and Authorisations Task

This section outlines the achievements of JRA3 T1 in the areas of distributed authorisation and group management, eduKEEP, standardisation work and dissemination.

2.1 Distributed Authorisation and Group Management

This section describes two key areas of achievement by the Distributed Authorisation and Group Management work item: multi-Attribute Authority (AA[1]) experiments using OpenStack and Moonshot.

2.1.1 OpenStack Multi-AA Experiment

2.1.1.1 *Introduction*

The goal of the OpenStack multi-AA experiment was to deploy an OpenStack [OpenStack] cloud in eduGAIN that is accessible using multiple Attribute Authorities (AAs) for authorisation. This would allow collaborations to manage their own groups and authorisations in their group management solution of choice.

This project required a number of software design decisions to be made. The most important of these was that OpenStack should be used in combination with production-level SAML middleware, so that proper handling of SAML-level actions was not demanded from OpenStack itself. This includes: (a) metadata handling – as per eduGAIN or other federation requirements – with signature verification, (b) handling of standalone AAs, (c) collaboration with discovery services, and (d) SAML single logout. As mentioned above, using OpenStack with production-level SAML middleware achieved the objective of reusing mature components without the need for building in SAML support itself. Moreover, it was important – to ensure efficient maintenance and development – that the new software should not be a patch to the OpenStack Horizon (dashboard) or Keystone (identity) components. Because of the encapsulation of the new functionality developed, no regular

[1] In the context of trust and identity, the abbreviation "AA" also/already has the meaning "Authentication and Authorisation". However, in the context of this document, it denotes "Attribute Authority" unless indicated otherwise.

patching of any other OpenStack components will be necessary, greatly simplifying maintenance and development support in future. The programming language Python [Python] and Django [Django] (a well-known Python web-application framework) were selected for consistency with other OpenStack components.

The solution needed to ensure that the user is always properly provisioned into Keystone before it makes contact with OpenStack. Otherwise the user would successfully log in to Shibboleth federation middleware, but would be denied access and greeted with an error message from Keystone since the user would not yet be known to Keystone. According to T1's design criteria, this meant that implementation in a hook of an OpenStack module should be avoided. As a result, the Task relied on the sessionHook ability of the Shibboleth SP.

2.1.1.2 *Main Workflow*

Figure 2.1 presents the main workflow of user provisioning using the newly introduced component called *regsite*. This workflow implements a collaboration between a SAML IdP, several SAML AAs, the SAML SP protecting Keystone, regsite, and, finally, Horizon (OpenStack's dashboard).

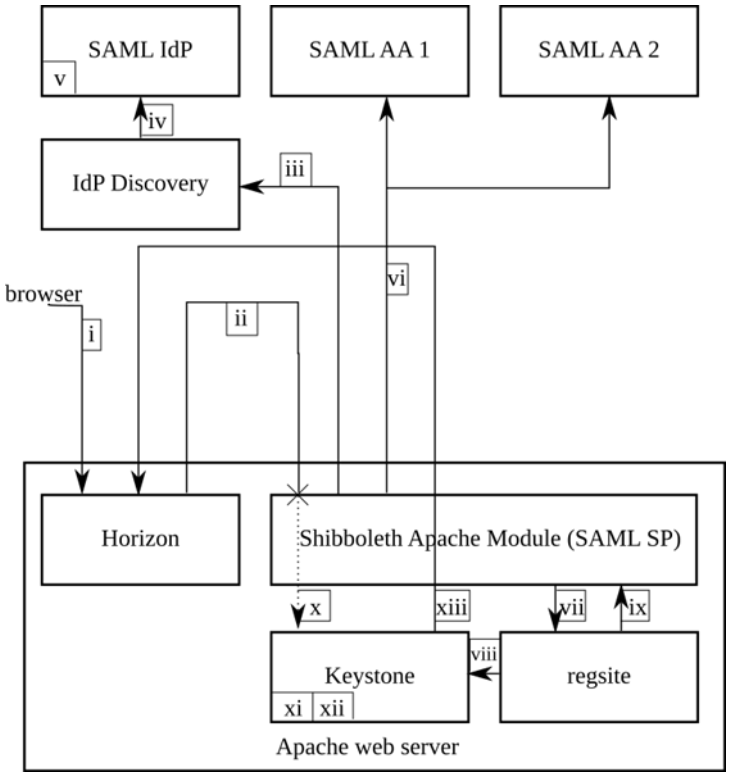

Figure 2.1: Main workflow of user provisioning (regsite component)

The workflow steps are as follows:

1. The user tries to access the OpenStack Horizon dashboard with a web browser.

2. Horizon redirects the user to the Keystone component's web endpoint.

3. The Keystone component is hosted by an Apache web server and is guarded by a Shibboleth SP. The user does not yet have a Shibboleth session, therefore a SAML login sequence is initiated. The user is forwarded to a SAML IdP discovery service, where s/he can select an Identity Provider.

4. The discovery service forwards the user to the Identity Provider selected by the user.

5. The user logs in at the Identity Provider using his/her home institution credentials.

6. Additional profile attributes and authoritative information is gathered from external attribute authorities, as defined by the Service Provider's configuration. The number of AAs contacted can range from 0 to many; however, the SP queries the AAs sequentially, which aggregates the round-trip times of the single queries. Meanwhile the user is blocked, which suggests that there is a practical upper limit to the number of AAs to be queried (as a rule of thumb, five AAs at most).

7. The Shibboleth SP merges and filters the received attributes, then executes its configured sessionHook. It forwards the user to a location hosted on the same server as the SP, which also relays all the attributes gathered during the login process. In sessionHook, the Shibboleth SP passes over the identity, profile and authoritative information to regsite. Steps (3) to (7) can all be completed by a standard Shibboleth SP.

8. regsite creates the user and the tenant[2], if necessary, using Keystone API calls.

9. regsite directs the user back into the Shibboleth login sequence.

10. The Shibboleth login sequence finishes, and the user finally reaches Keystone. The same set of information as was passed in step (7) to regsite is now passed in Apache Environment variables to Keystone.

11. Step (8) ensures that the user already exists in Keystone, as well as the tenants they are assigned to. Therefore, Keystone successfully authenticates the user.

12. Keystone creates a token for the user.

13. Keystone redirects the user to the Horizon web interface, accompanied by the newly created token. Horizon authenticates the user using this token and access is granted.

2.1.1.3 *Conclusions and Recommendations*

For the multi-AA experiment, the distributed authorisation team has deployed an OpenStack site [OpenStack-T1site] in eduGAIN, in which the user can authorise with either HEXAA [HEXAA], Perun

[2] A group of users within OpenStack. Also called a project. The terms project and tenant can be used interchangeably.

[Perun] or Grouper [Grouper], which are all group management and attribute authority solutions. The site is accessible for every eduGAIN user that has a Virtual Organisation membership in any of the AAs above. This OpenStack deployment works as expected, showing that the multi-AA solution created for OpenStack to perform user provisioning and access is completely successful.

Proposed and recommended future work includes a standard method for user-deprovisioning and standardisation of a scoped entitlement attribute, needed for proper authorisation without potential (scope) name clashes.

More information can be found in the white paper describing this solution [SAML-OpenStack-WP].

2.1.2 Moonshot Multi-AA Experiment

2.1.2.1 *Introduction*

The goal of the experiment was to create a proof-of-concept solution for demonstrating attribute queries to multiple AAs for non-web purposes. The planned process was as follows:

1. The end user performs Moonshot authentication with the Relying Party (RP) (in this case an OpenStack server with an Apache front-end) using its main IdP (in this case a RADIUS server) as usual.
2. As in any other Moonshot authentication, the Moonshot layer in the RP receives a SAML assertion from the authentication IdP.
3. Before providing the attributes to the application (i.e. the Apache front-end), the intention is that the Moonshot layer should perform a SAML attribute query to a second Attribute Authority (AA) using Transport Layer Security (TLS) and Simple Object Access Protocol (SOAP). In particular, the following requirements should be met:
    - The eduPersonPrincipalName (ePPN) attribute must be used to identify the end user in this query.
    - SAML SP metadata has to be exchanged with the AA in order to establish a secure SOAP channel.
    - The attributes received from the AA must be joined to those already received from the authentication IdP before being provided to the application.
4. The application obtains all the attributes.
    - The application should be unaware of the multi-AA process.

2.1.2.2 *Procedure*

To achieve the goal and planned process, the Task took as its starting point the results of the CLASSe project, where support for Moonshot-based authentication in OpenStack and Horizon was achieved. A description of how this integration was achieved can be found in the final report of the CLASSe project [CLASSe-FinalReport]. The essentials consist of enabling an extension in Keystone (called OS_FEDERATION) and protecting the IdP URL with mod_auth_kerb from the Moonshot project. Some additional modifications were required in the Horizon implementation, since at that time

(around the Juno release of OpenStack) the WebSSO interface was not yet completed and integrated into OpenStack.

For implementing multiple AA attribute queries – not present in CLASSe – the goal was to use the embedded Shibboleth SP support provided by the Moonshot libraries, preferably without modifying any of the Moonshot source code. After solving some packaging problems with the Moonshot Shib SP Resolver libraries, this turned out to be possible by following these steps:

1. Make the authentication IdP include the ePPN attribute of the end user in the SAML assertion delivered to the RP. Since the IdP in this (test) case is not actually connected to the eduGAIN fabric, a real ePPN needs to be set manually for the test users.
2. In the RP, modify Moonshot's shibboleth2.xml file to include the following configuration lines:

```
<!-Uses eduPersonPrincipalName from IdP to query other AA →
<AttributeResolver ty”e="SimpleAggregat”on" attribute”d="e”pn"
form”t="urn:oid:1.3.6.1.4.1.5923.1.1.”.6">
<Entity>https://hex aa.eduid.hu/hexaa</Entity>
</AttributeResolver>
```

3. Create a metadata file for the IdP and configure it in the RP, so that the RP accepts the ePPN as trusted information to continue with the queries towards the AAs.

4. Create metadata for the RP – including public key – and distribute it to the AA, so the AA trusts and answers attribute queries from the RP.

5. Configure AAs metadata in the RP, so the RP trusts the information coming from the AA.

After following these steps, the Moonshot layer in the RP is able to receive the attributes from the authentication IdP and the AA in a single SAML assertion. An example of a successful login using this setup is shown in Figure 2.2. However, Moonshot's original mod_auth_gssapi did not provide/transport the attributes it received onward to the Apache server; it only provided a single environment variable to the Apache server (REMOTE_USER) containing the end-user name as provided by the Moonshot layer. Any other attributes received were ignored and therefore did not reach OpenStack itself. After some modifications to mod_auth_gssapi, it was able to obtain the attributes from the Moonshot layer and export them as environment variables towards OpenStack. The resulting patch was provided to the Moonshot community as a contribution, which they used as a base to implement an improved version with more Apache configuration options.

2.1.2.3 *Results*

To test the final implementation described above, a publicly accessible web-based demonstration was set up with the deployment of an OpenStack server [OpenStackMoonshotDemo] that performs multi-AA queries to an operational HEXAA server [HEXAA]. Testing has shown that this OpenStack server is able to retrieve *entitlement* attributes from the HEXAA server, on which this OpenStack instance bases its authorisation decisions. The *entitlement* attribute is used to map the federated

end user into a particular group, assigning it to several protected projects (or tenants). All federated end users have access to the demonstration project, but only users with an *entitlement* attribute set to `urn:geant:niif.hu:hexaa:51:test1` are granted access to the SuperSecretProject project.

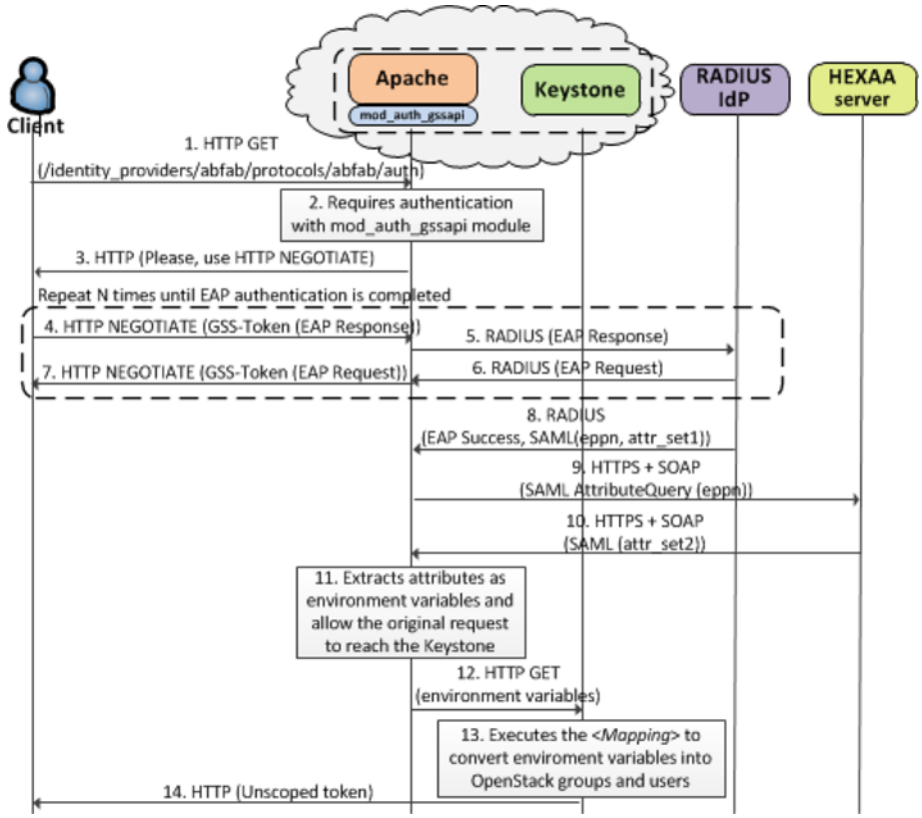

Figure 2.2: Federated authentication using Moonshot and support for multiple AAs

2.1.2.4 *Conclusions and Recommendations*

The experiment shows that it is possible to combine OpenStack with Moonshot and multiple AAs. One advantage of Moonshot is that a federated user can obtain tokens for use with a command line interface (CLI), effectively enabling CLI access to OpenStack. Authentication using the token should be possible using the cURL tool with GSS-API authentication. However, this tool has implementation issues that prevent it from using multi-roundtrip GSS-API authentication mechanisms such as GSS-EAP (the mechanism used by Moonshot). A small script written in Python that performs the GSS-API authentication with the Apache server can be downloaded from the OpenStack server public demonstration home page [OpenStackMoonshotDemo].

Similar to the OpenStack multi-AA experiment described in Section 2.1.1, proposed and recommended future work includes a standard method for user-deprovisioning and standardisation of a scoped entitlement attribute.

2.2 eduKEEP

2.2.1 Introduction

The goal of the eduKEEP work item was to study the implications of moving from an organisation-centric identity management model to a (more) user-centric identity federation model such as that provided by eduID developments in various federations. The description of the work in this section covers background, solution concept, architecture, example implementation, and conclusions and recommendations.

2.2.2 Background

eduGAIN interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation by coordinating elements of the federations' technical infrastructure and providing a policy framework that controls this information exchange.

Most, if not all, identity federations participating in eduGAIN manage users in an organisation-centric fashion, which has several implications, such as users who change organisations being issued new identities, even though they are linked to the very same person. Another implication is that if no suitable primary affiliation exists (for students leaving university, for example, or for research collaboration with industry partners), there is no straightforward 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.

Moving from an organisation-centric identity management model to a user-centric model would provide a solution for these cases, based on a long-lived Identity Provider where the user is in control.

2.2.3 Solution Concept

To achieve its goals, the eduKEEP concept leverages existing identity federations, thereby proposing a significant paradigm shift. The main changes in current architecture can be summarised as follows:

1. When retrieving a digital identity, two different processes intertwine: authentication and authorisation. eduKEEP makes a clear distinction between the two and distributes responsibilities within these two processes to the entities and organisations that can better commit to them.
2. In the complex ecosystem in which these processes are designed to operate, a digital identity will include information coming from different authoritative organisations or entities. Thus the processes to manage this identity need to interact – in a trusted and secure way – with different systems and subjects.

2.2.4 Architecture

In general terms, the process of a user accessing a service in this architecture has three distinct phases:

1. **The authentication phase**, in which the user interacts with different systems to prove he/she is who he/she claims to be. This will be the moment in which the user starts to retrieve his/her digital identity from the authenticating system.

2. **The identity enrichment phase**, in which the user will be guided through other, different systems to enrich his/her identity with additional information provided by other components of the architecture. This is the phase in which the digital identity, retrieved earlier, will be enriched and completed. The information retrieved will also include group memberships, roles and other important attributes that can be used by the service to enforce access rights to its resources.

3. **The service access phase**, in which the user will get his/her personal identity and present it to the service he/she wants to access to obtain the resources of interest. In this phase, the service has different options for consuming the information comprising the digital identity of the user. For example: presenting the identity to the service may include all the other attributes that make up the identity as well, or the service may get just the basic identity presented, and query for additional attributes afterwards, or a combination of both. In general, as little information as possible should be presented in the first step, since the service can always ask for more information if and when it is needed, e.g. for authorisation purposes.

The three phases are defined in a way that separates authentication from authorisation. The retrieval of the digital identity for the accessing user is a distinct phase from the enrichment of such an identity for authorisation purpose. Moreover, the architecture is based on the concept of a single enhanced identity for the user, with the user obtaining different pieces of information about his/her digital identity from different services and architectural components.

2.2.5 Example Implementation

The eduKEEP concept is not a single architecture, let alone one implementation, but a long-lived identity – or at least a long-lived identifier – with the capability of user-managed attributes as the key feature.

A possible implementation is shown in Figure 2.3, with a centrally managed IdP in which the user can manage his/her own data, which is enriched with data from other sources, such as entitlements and affiliations provided by various institutions.

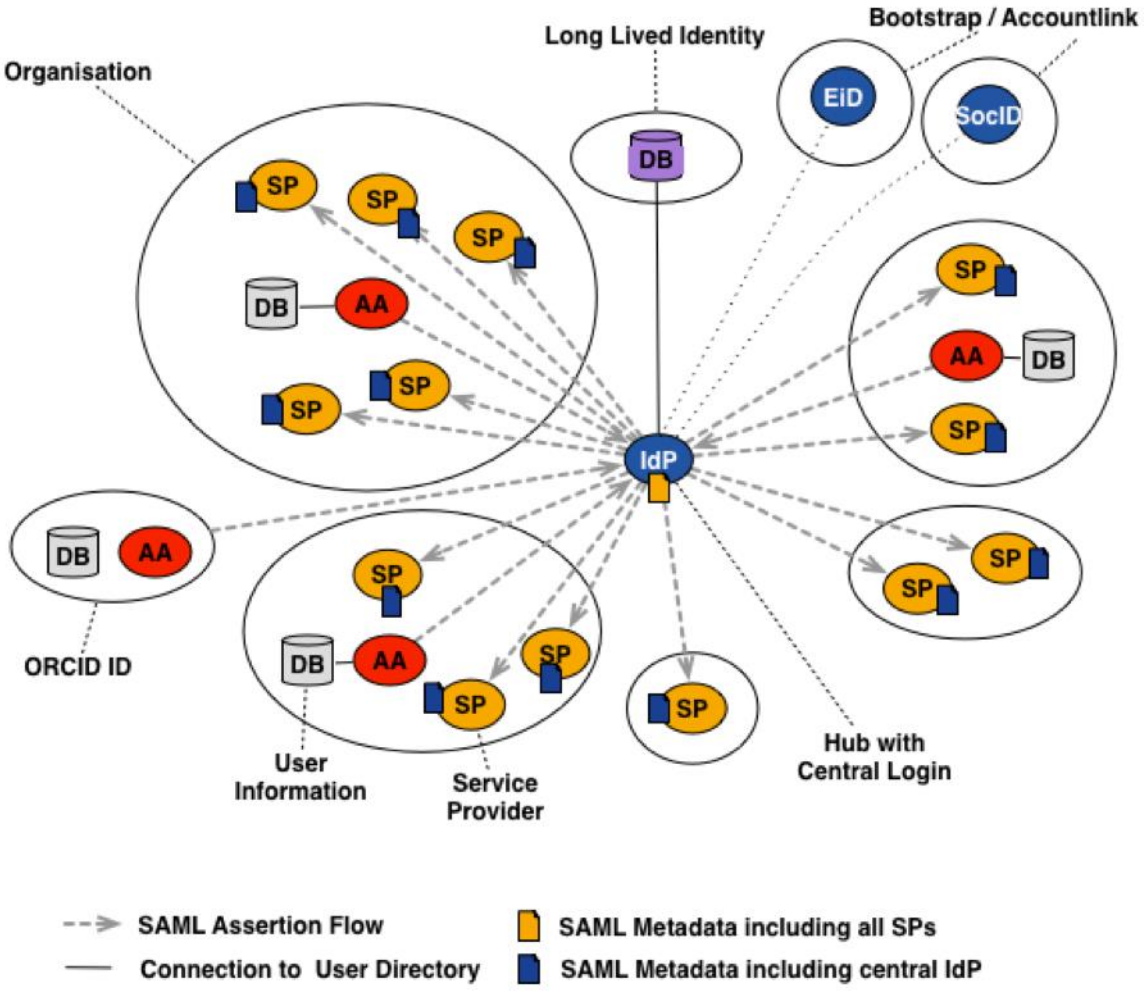

Figure 2.3: An eduKEEP architecture with a central IdP, containing identities enriched by other sources

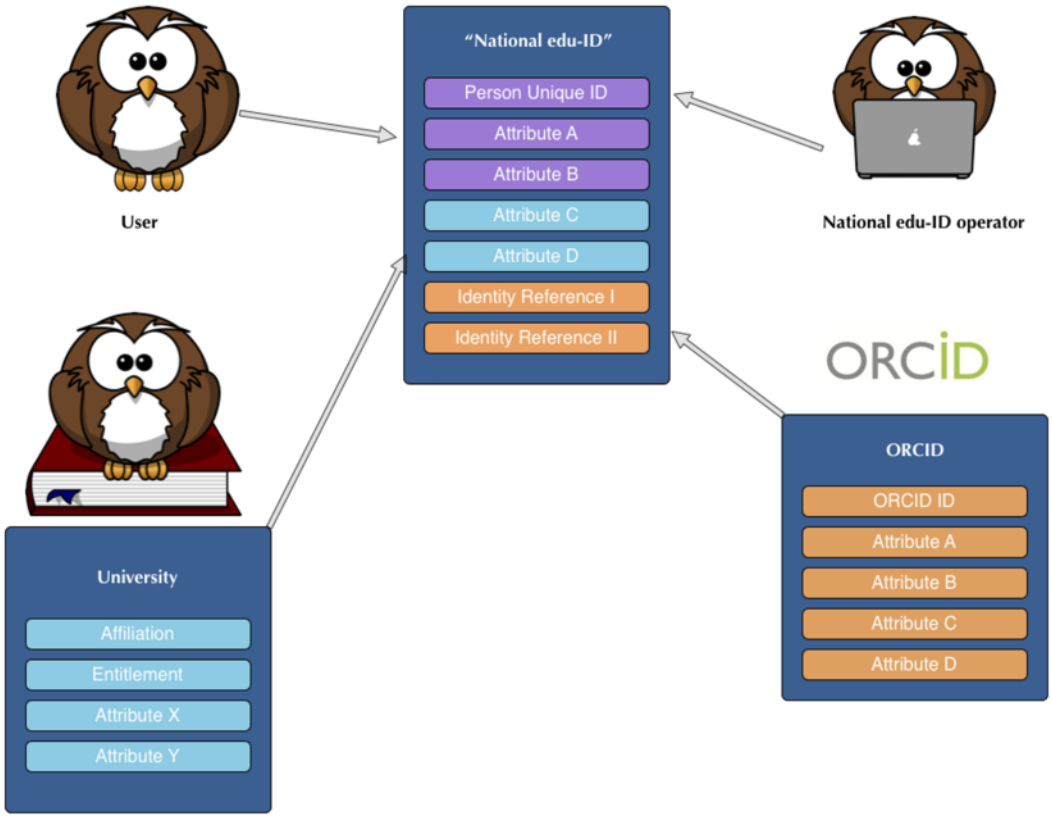

Figure 2.4: Combining attributes

When a user logs in at a Service Provider with his/her long-lived identity, the long-lived identity will be enriched by the additional resources that the user has linked to his/her (central) identity. This could be his/her ORCID identifier, and multiple entitlements and affiliations from multiple institutions as well as a verified address from the long-lived Identity Provider (Figure 2.4). Based on this rich set, the Service Provider can make an authorisation decision on the current set of attributes as well as make use of the attributes that the user allowed to be released to this SP (Figure 2.5).

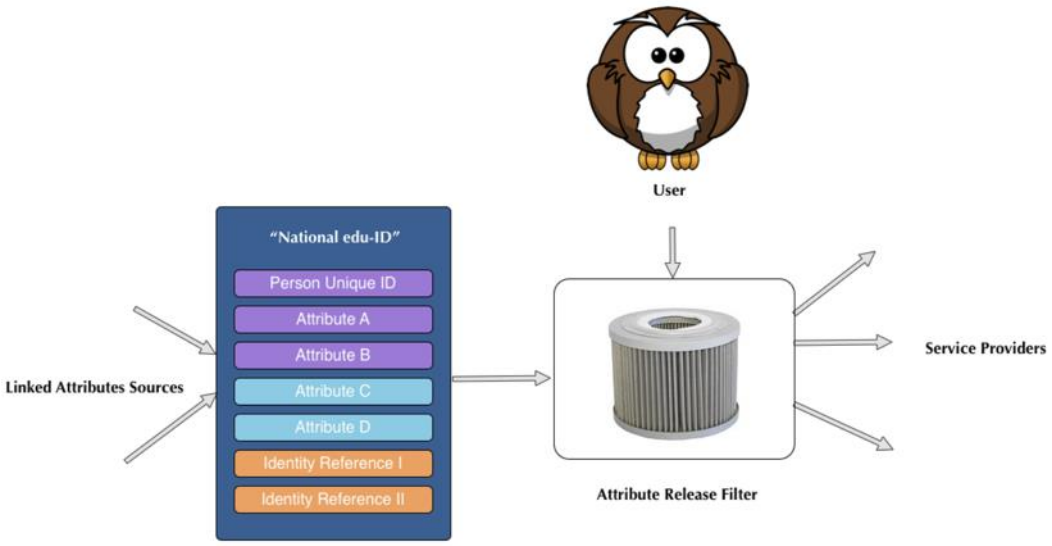

Figure 2.5: User-managed attribute release to a Service Provider

2.2.6 Conclusions and Recommendations

The conclusion drawn from this work item is that having a long-lived identity is a solid foundation on which to go forward with a (more) user-centric identity management federation model. The eduKEEP concept has been and will continue to be discussed at multiple conferences and meetings. It is the Task's recommendation that this work, together with the discussions, be used as input for the next phase of the GÉANT project and for NRENs on how to proceed with this paradigm shift in the R&E identity federation field and how to adjust and enhance the eduGAIN services to this new paradigm.

2.3 Standardisation Work

Although user consent for releasing attributes from Identity Providers is a feature common to almost all federations, so far the implementation of user consent has been tightly coupled to the Identity Provider implementation. User-managed access (UMA) – a standard developed by the Kantara Initiative [Kantara] – takes a different approach. It provides a unified control point where users themselves can determine who or what can get access to their data, regardless of the location where the data is stored. This approach ensures that consent management is decoupled from the Identity Provider itself. This also means that different IdP implementations and instances can use the same consent manager, or that a user can use one point to control attribute and information release for multiple identities he or she may have.

Two members of JRA3 T1 were actively involved in Kantara at the start of the project. However, personnel issues halfway through GN4-1 meant that priority had to be given to the work items in Task 2 of this Activity (Trust and Identity Technologies). With the specialised knowledge needed for involvement in this UMA work, it was not possible to find a proper replacement in time for the end

of the project; the Activity Leader therefore decided to postpone this work item until the next phase of the project.

2.4 Dissemination

Table 2.1 below shows the main dissemination activities JRA3 T1 has undertaken during GN4-1 to present, raise awareness of and encourage discussion about its progress and achievements. It is recommended that the level of activity be maintained, particularly with regard to eduKEEP, to elicit input as to its future development.

Type	Title	Event	Location	Date	Link
Presentation	OpenStack SAML Integration with HEXAA	OpenStack CEE Day 2015	Budapest	08-05-2015	http://openstack.hexaa.eu/
Presentation	Federated Authorisation	TNC2015	Porto	16-06-2015	https://tnc15.terena.org/core/presentation/89
Presentation	InAcademia Simple Validation Service	TNC2015	Porto	16-06-2015	https://tnc15.terena.org/core/presentation/111
Journal paper	Collaboration between SAML Federations and OpenStack Clouds	International Journal of Cooperative Information Systems	N/A	14-10-2015	http://arxiv.org/abs/1510.04017
Presentation	eduKEEP	Internet2 TechExchange	Cleveland, Ohio	07-10-2015	http://meetings.internet2.edu/media/medialibrary/2015/10/16/20151007-Kremers-eduKEEP.pdf
Presentation	OpenStack and SAML Integration + OpenNebula Multiple AA Integration	Workshop on Federated Identity for Cloud Services	Zürich	21-01-2016	https://wiki.geant.org/download/attachments/53117373/Cloud_AAI_workshop_Heder.pdf

Table 2.1: Dissemination activities

3 Conclusions and Recommendations

To summarise the conclusions and recommendations for the areas of work undertaken by JRA3 T1 during GN4-1:

- The OpenStack multi-AA solution that allows the user to authorise with a variety of Attribute Authorities (AAs) to perform user provisioning and access was successful.

  It is recommended that future work includes a standard method for user-deprovisioning and standardisation of a scoped entitlement attribute, needed for proper authorisation without potential (scope) name clashes.

- The Moonshot multi-AA experiment showed that it is possible to combine OpenStack with Moonshot and multiple AAs. An implementation issue that was preventing CLI access to OpenStack (using scoped tokens, the cURL tool and GSS-API authentication) has been addressed with a small, publicly available Python script.

  The same recommendations as for the OpenStack multi-AA solution apply to this experiment: future work should include a standard method for user-deprovisioning and standardisation of a scoped entitlement attribute.

- The eduKEEP work item has shown that a long-lived identity/identifier is a solid foundation on which to build a (more) user-centric identity management federation model.

  It is recommended that this work, together with ongoing discussions with interested parties, be used as input for the next phase of the GÉANT project in respect of how to proceed with this identity federation paradigm shift and how to adjust and enhance the eduGAIN services accordingly.

- Initial work on a new, user-managed access standard has been shown to deliver significant benefits.

  Resourcing issues and reprioritisation during GN4-1 meant that development work could not continue. However, it is recommended that the work be resumed in the next phase of the GÉANT project.

- JRA3 T1 has carried out several high-profile dissemination activities during GN4-1, including at TNC2015 and Internet2 TechExchange.

  It is recommended that the level of activity be maintained, particularly with regard to eduKEEP, to elicit input as to its future development.

References

[CLASSe-FinalReport]	A. Perez-Mendez, R. Marin-Lopez, G. Lopez-Millan, D. W. Chadwick, *Open Call Deliverable OCD-D1.2 Final Report (CLASSe)* http://geant3plus.archive.geant.net/Resources/Open_Call_deliverables/Documents/CLASSe_final_report.pdf
[Django]	https://www.djangoproject.com/
[Grouper]	https://grouper.idem.garr.it/grouper-sp/en/info.html
[HEXAA]	https://hexaa.eduid.hu/hexaa
[Kantara]	https://kantarainitiative.org/confluence/display/uma/Home
[OpenStack]	https://www.openstack.org/
[OpenStackMoonshotDemo]	http://moonshot-multiaa.inf.um.es
[OpenStack-T1site]	https://openstack.hbit.sztaki.hu
[Perun]	https://edugain-group.cesnet.cz/idp/shibboleth
[Python]	https://wiki.python.org/moin/FrontPage
[SAML-OpenStack-WP]	M. Heder, S. Tenczer, A, Biancini, *Collaboration between SAML Federations and OpenStack Clouds* http://arxiv.org/abs/1510.04017

Glossary

AA	Attribute Authority[3]
AAI	Authentication and Authorisation Infrastructure
ABFAB	Application Bridging for Federated Access Beyond web
API	Application Programming Interface
CEE	Central and Eastern Europe
CLASSe	Cloud-ABFAB Federation Services in eduroam (GN3plus Open Call project under the Authentication theme)
CLI	Command Line Interface
CMS	Content Management System
cURL	A command-line application for performing requests using a variety of protocols including HTTP
EAP	Extensible Authentication Protocol
eduGAIN	EDUcation Global Authentication INfrastructure
eduID	A system that allows lookup, verification and assignment of unique identifiers for the R&E community
eduKEEP	An architecture model developed by GÉANT that aims to transform current identity federations to provide a user-centric approach for managing digital identities
ePPN	eduPersonPrincipalName (attribute containing a scoped identifier of a user, in the form user@scope)
FAM	Federated Access Management
Grouper	An enterprise access management system developed by GARR, designed for environments with highly distributed management and heterogeneous information technology such as universities
GSS-API	Generic Security Services API
GSS-EAP	GSS-API mechanism for the Extensible Authentication Protocol
HEXAA	Higher Education External Attribute Authority
IdP	Identity Provider
IETF	Internet Engineering Task Force
JRA	Joint Research Activity
JRA3	GN4-1 JRA3 Trust and Identity Research

[3] In the context of trust and identity, the abbreviation "AA" also/already has the meaning "Authentication and Authorisation". However, in the context of this document, it denotes "Attribute Authority" unless indicated otherwise.

Moonshot	A technology developed by Jisc, based on the IETF's ABFAB open standards, which aims to enable federated access to virtually any application or service
NREN	National Research and Education Network
OpenStack	A free and open-source software platform for cloud computing, mostly deployed as an infrastructure-as-a-service.
ORCID	An open, non-profit, community-based effort to provide a registry of unique researcher identifiers and a transparent method of linking research activities and outputs to these identifiers
Perun	An open source identity and access management system
R&E	Research and Education
RADIUS	Remote Authentication Dial-In User Service (an Authentication and Authorisation protocol)
RP	Relying Party (synonymous with SP)
RPC	Remote Procedure Call(s)
SP	Service Provider
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol (an XML-based RPC mechanism)
SSO	Single Sign On
T	Task
T1	Task 1 Attributes and Authorisations
TLS	Transport Layer Security
TNC	The Networking Conference
UMA	User-Managed Access
URL	Uniform Resource Locator
VOOT	Virtual Organisation Orthogonal Technology
WebSSO	Web Single Sign-On (browser-based SSO)