eduKEEP

Towards a user centric identity federation

20 April 2016

Maarten Kremers, SURFnet maarten.kremers@surfnet.nl
Andrea Biancini, Consortium GARR andrea.biancini@garr.it
Davide Vaghetti davide.vaghetti@garr.it
Marco Malavolti, Consortium GARR marco.malavolti@garr.it
Christoph Graf, SWITCH christoph.graf@switch.ch
Rolf Brugger, SWITCH rolf.brugger@switch.ch

Introduction

The goal of the eduKEEP work item in the GN4-1 project 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.

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.

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.

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.

1.1 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 1, 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.

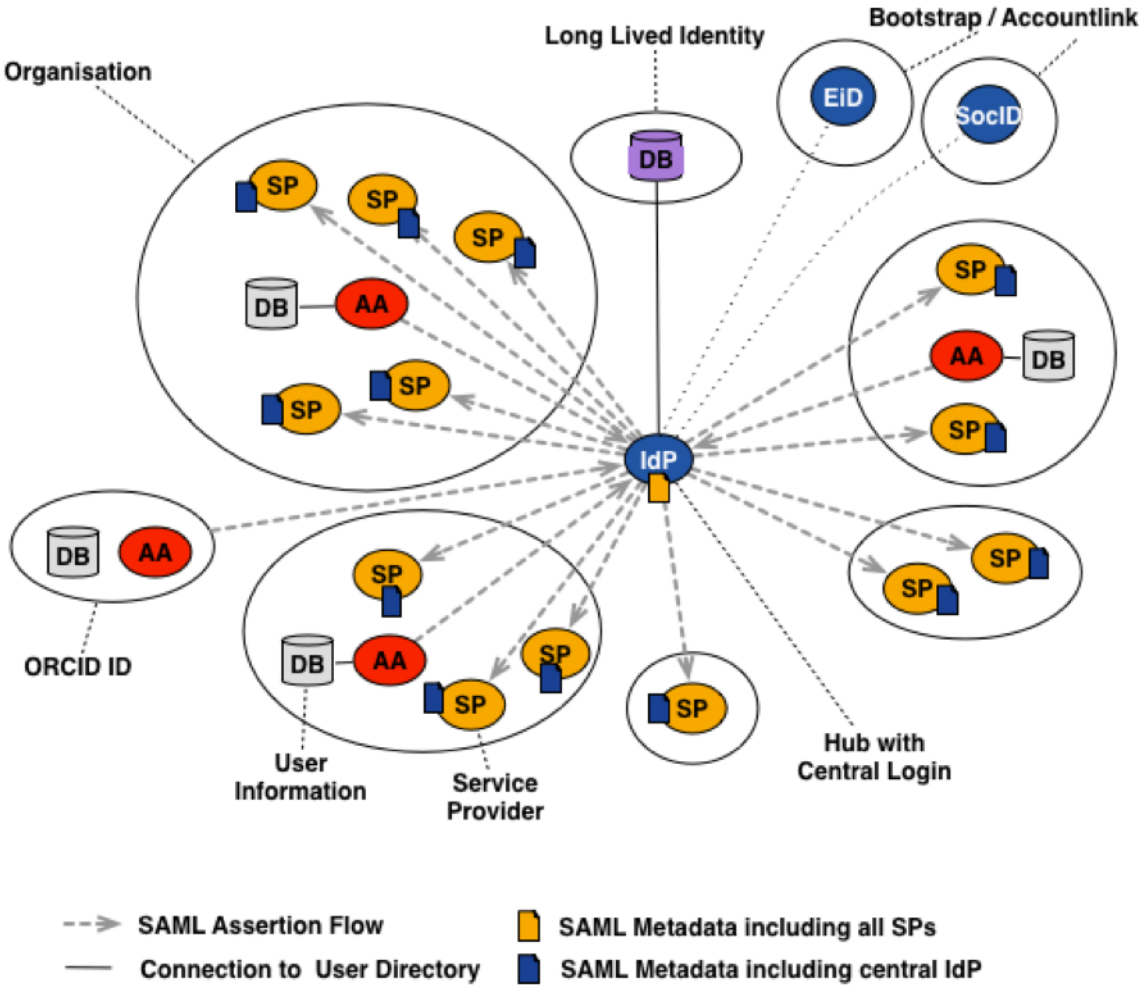

Figure 1: An eduKEEP architecture with a central IdP, containing identities enriched by other sources

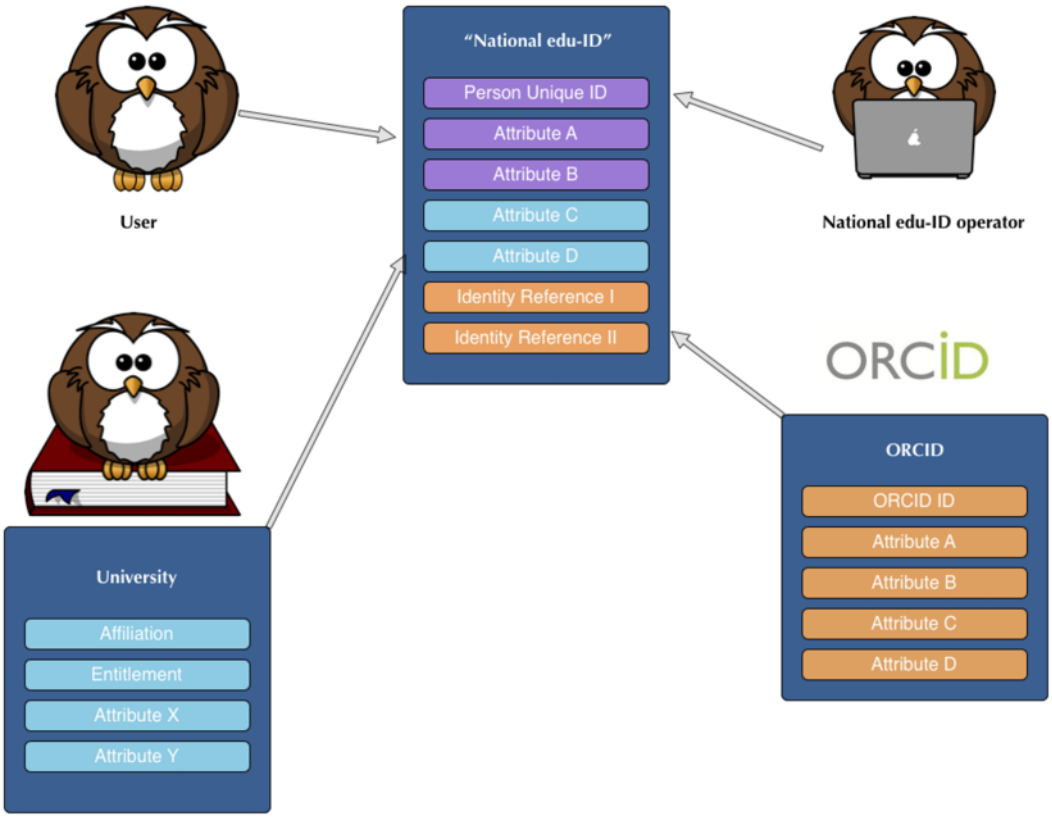

Figure 2: Combining attributes

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). 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 3).

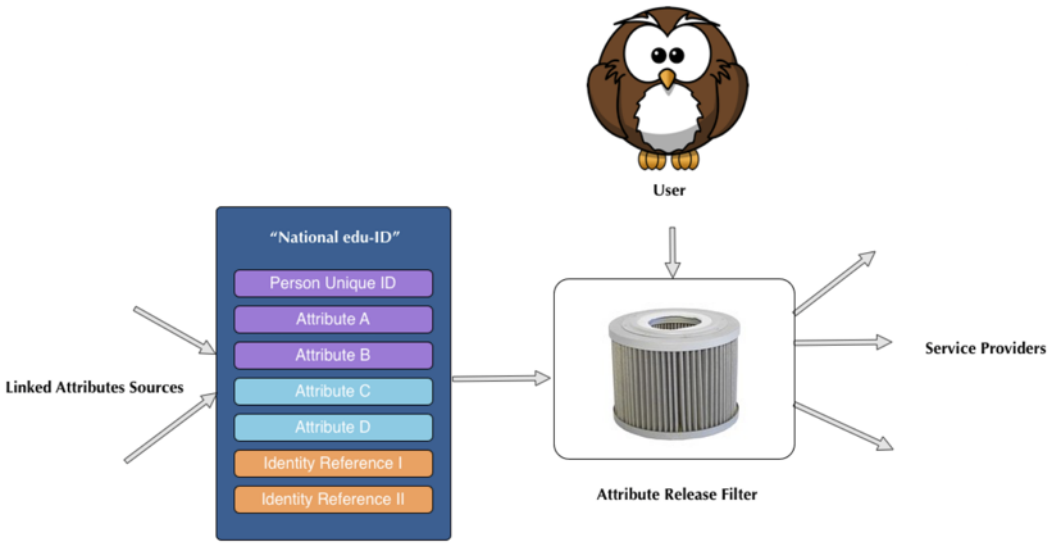

Figure 3: User-managed attribute release to a Service Provider

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.

Acknowledgement

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