Call with the NRENs on the European Student Identifier

Date: 4th October 2019

Introduction

Licia briefly introduced MyAcademicID project. The project which is led by EUF (European University Foundation) aims to enable student mobility by enabling federated access for some of the Erasmus tools and services. GÉANT, SUNET and RENATER participate for the NREN/Fed-Ops community.

Erasmus student mobility keeps growing steadily over the years, and funding has been made available to automate the process. At the moment, the online tools and services that are available to support student mobility and the exchange of the student grades are not federated. The technical aspects to enable federated access for the Erasmus tools are underway as part of MyAcademicID project; it is however important to note that universities will keep using some out of band mechanisms to exchange students grades.

The main use-case (and challenge) is how to enable federated access to the identified Erasmus services (via eduGAIN); at the same time we need to ensure that a user is unequivocally identified, starting from the moment he/she logs in via eduGAIN/national federation to fill-in the online application, until his/her participation in the Erasmus program is completed. . During this lifecycle, the user will have to access numerous online services, data records will be transferred from his/her University to Erasmus and the receiving University, and the user while at the receiving University should be able to receive services, such as accessing the campus canteen etc, using his/her European Student Card.

In order to enable this, the student will have to have an identifier that will be used to unequivocally identify him/her across service and when his/her student records are exchanged as part of the Erasmus process. The Identity Management Systems behind the Identity Providers at the campuses, do have such identifiers for each user account, but in many cases these identifiers are specific to the IT services and are not linked with identifiers used in the student records or in the university student cards.

There is an opportunity to work together to expand the reach of federated access actively contribute in enabling the Erasmus programme and student mobility in Europe.

Aim of the call

The aim of the call was to discuss if and how federation operators can play a role in supporting the identifier needed for the use-case highlighted above. A subset of federation operators have been invited to join the call. Christos presented the work done so far as part of MyAcademicID as well as work that happened prior to MyAcademicID.

There are different identifiers but none of them alone would solve the challenge above. The main requirements for such an identifier are:

- Globally Unique: Each student should be uniquely identified across organizational and national boundaries
- Persistent: The identifier should follow the student during her/his time of studies
- Non-targeted: The identifier should be the same for all services involved in the student mobility processes
- Protocol neutral: The identifier should not change value depending on the propocal used. For example, it should be the same regardless is SAML or OpenID Connect is used
- Data transport neural: The identifier should not change value depending on how it is transported. For example, the students should be identified by the same identifier regardless if it is through a federated authentication flow or a back-channel transfer of records.

Looking at the existing identifiers:

- ESI (European Student Identifier) - this identifier was created prior to MyAcademicID project as result of other EC funding led by CNOUS. ESI structure (agreed a few years ago) resembles an IBAN code, and encodes the institution as well as the student identifier. There are some challenges with this identifier: one of the biggest is that atm to identify the institutions it uses a code that is maintained by the EC and will be discontinued shortly.
- SCHACUniqueID could be used as a transport mechanism but we would still need a way to uniquely identify the institution. Also SCHAC is not widely deployed
- eduPerson ePTID and ePPN: widely used in the HE federations. However ePTID is targeted and thus will change from one service to the other, while for ePPN there is no guarantee that it will not be reassigned. Also they do not necessarily link to the student identifier that follows the student record.

How can federations help?

Q: ESI seems to carry a lot of information, how do we keep it unique? I.e. a users start at institution A then move to B, then the identifier would changes The identifier of the institution could be send via the federated access).

Q: Is the organisation sent via IdP the same info that is used for Erasmus purposes?

A: Joao noted that for some Erasmus services to work, they need to verify the institution. The users could provide that but that would generate more errors. The proposed format was to support different situations where some countries manages the student numbers centrally, and some others do not.

ESI contains the student number + the organisational code - The latter needs changing as the EC will replace the current format which is used to identify institutions applying for grants. In fact it would be desirable to allow for different type of organisational codes. The student number, which is managed by the student's home organisation, is in most of the cases not encoded in the IDM systems of the universities.

The Fed Ops can help by:

- Joining the discussion on the evolution of the ESI
- Working together to define how to encode and transport the organisational identifier
- Working together to agree how to encode the student number in the IDM systems.

Leif noted that together with Victoriano they are looking at the scalable ways to uniquely identify the users' organisations. The ideal solution would be a globally unique way of expressing the academic records of a given person in such a way that the identifiers can be resolved back to the accrediting institution in a secure way that prevents forgeries and spoofing.

There are standards being specified that could achieve the proposed solution, like DIDs (Distributed Identity Document) and VCs (Virtual Credentials), but this will require substantial changes in how things are done in the current identity and data federations in Higher Education. It was agreed however that a short term solution is needed and that an incremental approach to solving the problem should be found.

Next steps

It was agreed to start with a practical approach before migrating to a more complex solution.

As a first approach, current Higher Education Federations in eduGAIN could be leveraged. Federation operators could ask IdPs to add both schacHomeOrganization and schacPersonalUniqueCode to IdP metadata distributed through the federations metadata feed.

schacHomeOrganization would be used to carry the internet domain for the institution the IdP belongs to. And schacPersonalUniqueCode will be multivalued and carry the institution identifiers (whatever they may be).

Victoriano proposed to find a way to use an identifier that is encoded as SCHACPersonalUniqueCode and also includes the SCHACHomeOrg following this format:

urn:schac:personalUniqueCode:es:uma.es:estudiante:1234567

This proposal should be further discussed and a plan on how to test should be agreed upon as soon as possible (a new doodle will be sent soon).

Miro volunteered to test in Croatia.