eunis dublin 2011

EUROPEAN UNIVERSITY INFORMATION SYSTEMS

eunis
International Congress
Dublin, Ireland,
Wed 15th - Fri 17th June 2011

Maintaining a sustainable Future for IT in Higher Education

Wednesday 15th June 2011

Time: 11:30 - 12:00

How Many Are You?

“How many are you?” seems a silly question but in the daily practice of universities a lot of persons have multiple digital identities.

First it is necessary to distinguish a role from an identity: multiple roles are a common practice in identity and access management. Different identities are based on the different sources where identities have their base. Roles are based on attributes of a person.

Staff members have their base in the registration in the HR system, students in the student administration, alumni sometimes in the student administration, sometimes in an independent alumni administration and often a kind of affiliate registration is used for guests or people who are temporarily doing some work for a university department.

Most people belong to only one category: a staff member, a student or an alumnus. Often a person is a student and staff member, a staff member and alumnus, and sometimes even student, staff member and alumnus simultaneously.

All these registrations enter the university directory and in most cases people get multiple identities depending on the source system of their registration.

This means that they should constantly be aware of which identity they use in a specific circumstance, for a staff member can use a system in one way, a student must use it in another. Also the environment - colleagues and fellow-students - should be aware who they address: the student or the staff member.

The question we want to discuss here is the possibility to give these people just one identity. A lot of questions pop up:

- Is it possible to match persons from different source registrations?
- What does this mean for the provisioning to applications?
- How about Deprovisioning?
- Does it generate a security problem?
- etc.

Why should you want to avoid multiple identities? It is more user friendly for the persons concerned and, since we have roles, why should being a student, an alumnus or a staff member not be a role like any other role? If we are so driven to role based identity and access management, why is being a student, staff or alumni not a role?

First, let's explore the possibility to **match people** from different source systems. For simple matching a unique identifier per person is the easy way. But does such a unique identifier exist, and if so, can we legally use that? Is this identifier registered in all source systems?

If not, how to match? How "sloppy" are the registrations? Are (all of) the officially names registered? Can or should we use date of birth? How do we deal with twins?

If manual labour is needed to make the perfect match, who is going to do it en how much time is involved?

And when the match is made, what are the consequences for the entry of this person in the directory? Does the schema of the directory need adjustment? If so, how?

Next, let's have a look into **applications** where different categories have different roles. For instance electronic learning systems and education information systems have very different roles for students and staff. Staff members can grade students; students can only look into their grades.

Are those applications fit for role based access? If not, what to do about it. Special attention is needed for self service applications. Who is the "self" here, the student or the employee identity, and what are his or her rights?

Furthermore, how to manage **provisioning** and **deprovisioning**? To deprovision a role instead of deprovisioning an identity requires a different approach. Will deprovisioning become more complex, is it possible?

And last but not least, will this generate a **security** problem? Does this give opportunities for abuse?
Delft University of Technology is looking into these questions and has some tentative answers:

- It is possible to **match people** but the challenge is to minimize the manual actions. One registration should be defined as the authoritative source.
- For **applications**, who distinguish different roles for staff and students there are two possibilities

    - Roles and the necessary data for these roles will be provisioned and the user can interact according to the role he chooses.
    - The application has different entries (for instance URL's) for different roles. The data for the roles will be provisioned and the user chooses the entry of the role with which he wants to interact with the application.

  Attention is needed for self service applications, especially the applications where the user can change his or her own data. The authoritative source of the data is very important in this situation.

- Provision of data to other applications will not be so very different; the changes of roles will be important triggers instead of the presence in a HR or student administration. **Deprovisioning** of identities will in some cases be deprovisioning of roles.
- There will be no new **security** problem when we use only one digital identity. Using roles in stead of different identities doesn't increase the risk for abuse.

We will present the results and illustrate the choices we made.