

Identity Based Clusters of Applications for Collaboration and eLearning

José A. Accino¹, Manuel Cebrian² and Victoriano Giralt³

¹Central ICT Services, University of Málaga, Blvd. Louis Pasteur 33, Malaga, E29071 Spain, accino@uma.es. ²Faculty of Educational Sciences, University of Málaga, Blvd. Louis Pasteur 4, Málaga, E29071 Spain, mcebrian@uma.es. ³Central ICT Services, University of Málaga, Blvd. Louis Pasteur 33, Malaga, E29071 Spain, victoriano@uma.es.

Keywords

Identity, federations, collaborative applications, SAML, OKI.

1. EXECUTIVE SUMMARY

There is a growing perception that the old model for environments of collaboration, like those used in eLearning platforms, is failing under its own weight. This approach could be named as *application centric* and might be defined as “trying to enrich the user experience providing the platform with every feature that could be thought of.. and then some” (a.k.a. Kitchen sink syndrome). This is also true for other closed environments like groupware collaboration suites. This approach has close links to a desire of the given platform becoming dominant in the market as the easiest solution to the integration problem. Thus, environments develop into specific universes with their own access rules, authorization, resource management, communications - chat, mail - and so on, which has important shortcomings. The concept of a “dominant platform”, due to the size of the scene, is neither feasible nor desirable, as it is neither viable, not even in the medium term, an unlimited growth of components and modules that replicate already existing functions from other tools.

Also, there is an increasing need for a paradigm change in collaborating platforms, like those used for eLearning. And the conditions for such a paradigm shift do exist. This new paradigm should be centered around the user, facilitate collaboration both amongst users and applications themselves and should reflect more closely the daily experience users have when using *the Net*. The technology that will enable this paradigm shift is Federated Identity and Access Management (IAM). This *user centric* design is focused on making platforms more permeable, transforming them into a fuzzy delimited environment without hampering security. Interoperability is key: “Interoperability is the degree to which a provider and consumer can successfully interface having never met” or, rephrasing in more modest terms, collaboration between applications. I.e.: Transforming applications from a model resembling a flat with walls and doors into a seamless loft.

This paper will describe the present status of the works developed over several years both within the Agora Sur research group -and its test bed *Ágora Virtual eLearning environment*- and the Central IT services of the University of Málaga. These developments revolve around the concept of *application clusters*, a group of applications that share a common Authentication and Authorization Infrastructure and allow groups of loosely (or tightly) coupled people to achieve a common goal. One of these clusters is being deployed to support presence learning in our university.

2. INTRODUCTION

On the present paper, we will be discussing on what seems to be a new way of looking at teaching and learning tools and services for our universities. Universities offer services and tools to support the learning process. These services and tools should be integrated with the rest of supporting services, like, for example, student registration systems. Enterprise Application Integration (EAI) is not an easy task. Most applications have their own information repository that has to be, in the best case, provisioned out of enterprise data, in the case of universities, the academic management systems. The most common *solution* up to this moment has been a monolithic platform with just one information repository to provision, but, at the same time, with just one way of doing things, *their own*.

To be honest, this is not really a solution. Monolithic platforms cannot compete with the gamut of available good tools that evolve at a much more rapid pace. This translates into the institution being held hostage of an environment, be it free (FOSS) or proprietary. Think about the problems that platform migration poses to IT system administrators, not to talk about down time, extended projects, lifetime extensions of the old one, parallel runs, and such.

The network expands its reach daily and users start to use it at increasingly earlier ages, which means that most university students arrive having a previous technological background, that has often been self-taught.

It is more frequent that students and, even, a significant number of the university personnel have their own free e-mail accounts and they use them in preference to the institutional ones, as they also prefer using their usual instant messaging tools, that fulfill most of their communication needs. Users want to easily and seamlessly share their resources as they do in their daily experience of the network with their bookmarks, images or documents. Thus, what is inside the academic environment cannot remain aside of the rest of the world. Users do not want to be confronted to multiple authentication processes, diverse passwords, application specific search tools, or communication tools different from the ones they are used to use.

The use of an integrated, monolithic learning platform, under this circumstances, becomes another compulsory task that extends the separation between personal and academic contexts into the network, thus reducing the possibility of a really user centric learning. So, we wonder if labeling some platforms as more or less *constructivist* (fashionable term in pedagogical papers) than others, as real daily practice is not different from traditional presence learning models.

So, we are going to present our way of achieving an identity centric learning environment using modern technologies for identity federation that allow us for that paradigm shift. Then the present paper is of use for both technical IT people supporting learning environments and the education experts that use them to get a head start of a proposed new paradigm..

3. DESIGN ALTERNATIVES: APPLICATION CENTRIC VERSUS USER CENTRIC

The process for integrating the user experience outside the learning environment in order to enrich it has both wide pedagogical implications as design and technology election ones. The most commonly used alternative is that we refer to as application centric design. We could define the paradigm for this methodology as “trying to enrich the user experience providing the platform with every feature that could be thought of.. and the some” (a.k.a. kitchen sink syndrome). Thus, learning environments develop into specific universes with their own access rules, authorization, resource management, communications - chat, mail - and so on, which has important shortcomings.

The reader has probably been confronted sometime with the problems associated to the deployment of one of this environments inside an institutional infrastructure, like the ones that derive from the integration of other applications inside said environment or the ones related to student management: the former usually require an application rewrite to some extent (as happens with OSP in Sakai) or the use some concocted mechanism that result in a n integration that is more perceived that real (e.g. LAMS in Moodle); the later have no other solution that devising some mechanisms that keep the diverse databases in sync or multiply the data entry processes.

The second alternative, that we designate as user centric design is focused, on the other hand, on making platforms more permeable, on transforming them into a fuzzy delimited environment, like the network experience is, without hampering security. This means wondering which are the most adequate architectures when the desired result is placing the user in the middle of his diverse experiences, in all, it is the same as talking about identity centered architectures and applications that collaborate amongst themselves.

The selection of technologies for the works presented here have been made on the basis of simplicity, that being that their deployment does not require a significant amount of technical expertise in not too extended technologies, this meaning that most of the presented architectures are very easy to deploy on top of widespread infrastructural software like Apache and PHP, require few other things, apart from the obviously existing services in any academic environments like universities (student registration and suchlike). Seamless integration of elearning environments into normal academic environments already in place for presence learning is key to an easy transition into a the new model that will be most probably be required in the coming years for many levels of education, specially in Europe with the implementation of the Bologna process guidelines.

Technologies that are difficult to the deploy, or require specially concocted procedures to get corporate information fed into them, face a serious risk of not being used due to many reasons, scarcity of trained experts and economies of scale not being minor ones.

4. ÁGORA VIRTUAL®: A SAMPLE OF EVOLVING ARCHITECTURE

We presented Agora Virtual® in 2006 as a collaborative platform, giving the term a dual meaning: an environment for user collaboration and also a platform that works with other applications and services to minimize the need for any wheel reinvention.

This way of working included, for example, an initial implementation of the authentication OSID, using Google Maps API for one of the modules or an external Jabber server as instant messaging server (jabberd2 at first, now Openfire), but other modules are still in the old traditional format, like the Rubric one, developed as a way of experimenting the use of formative evaluation in big groups along the lines defined by EEES.

Once the platform has reached an adequate level of stability, after two years of intensive use in several projects and formative activities, the authors thought about future development for advancing in the above direction, and identified two models that are equivalent to the already described design alternatives; i.e., follow a tool centric model and start an endless race of gadget additions or, on the other hand, evaluate how to centre the current architecture around the user, working in two closely related areas: collaboration amongst applications and identity technologies.

5. INTEROPERABILITY AND IDENTITY: OKI-OSID + PAPI + SimpleSAMLphp

It should be stressed that the technologies we are presenting here can be used in many environments inside and outside education, as shown by the raising interest in identity federation technologies. Identity fragmentation is one of the most prominent issues that users are facing, they are the same person whichever service or application they are using and a sea of credentials for accessing them does contribute neither to usability nor to security. Thus, any technology that can be used to reduce this number of credentials, is worth the efforts even if they require a paradigm shift from the established status quo. Once this principles have been laid out, we will present how we have applied them to evolve an existing elearning platform in use for several years into an identity centric learning environment.

OKI project OSID (Open Service Interface Definitions) are a set of specifications that define how the different components of a software environment communicate with each other and with other systems. Ágora Virtual® has used its own implementation of the authentication OSID - and its required OSID like Shared - since its first version, thus the next step for increasing its interoperability is extending OSID to the rest of modules and functions.

The Campus Project, backed by the Generalitat of Catalonia and eight Catalanian universities, goes along the same lines of thought, though their approach is to connect the existing platforms, like Sakai or Moodle, to the OKI bus, instead of substituting the platform by a bunch of applications that

collaborate, thanks to a shared identity, over said enterprise bus. Anyhow, we are very happy to find that there is a big potential for collaboration between both projects.

Agora Virtual® present architecture defines a single point of authentication and authorisation in the application front controller, and this eases the integration with external mechanisms.

SimpleSAMLphp is a light PHP library based on Sun's OpenSSO Extensions (a.k.a. Lightbulb) that permits any service developed in this language to easily integrate into any SAML based identity management infrastructure. The most common way of deployment of a SAML 2.0 SP (Service Provider) is to use an interface written in the same language as the application, for easy communication between it and the SP (see figure 1). It is even possible to build interfaces for protecting applications in other languages, using facilities provided by SimpleSAMLphp for passing attribute information out of band.

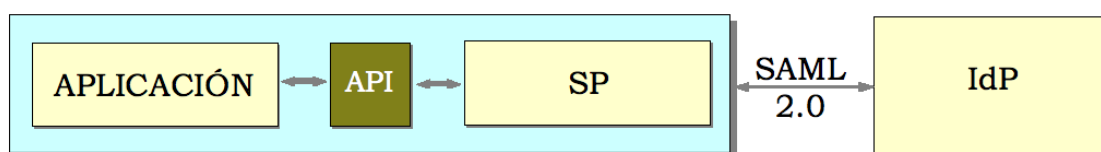


Figure 1. SimpleSAMLphp implementation

PAPI is a federation protocol and infrastructure based on a very simple model of trust. This trust is just one way, different from the two way trust that is common in SAML based federations. We should explain some of the terminology in order to understand how this trust model works.

- Point of Access or PoA is both a protected resource and a piece of code to protect it.
- Groupwide GPoA is a common trust anchor for a group of protected resources (PoAs)
- Authentication Server or AS is the point where user authentication occurs.

The AS can be substituted by any other mechanism for protecting the resource and gathering attributes, like a SAML Service Provider. This has allowed our mixed environment design. SAML allows integration into identity federations, PAPI allows for easy and fast deployment of trusting applications.

The phpPoA design requires a GPoA that communicates with the IdP (SimpleSAML in our case). We have a modified GPoA, called SimpleSAMLGPoA, that acts as a hybrid component that creates an encrypted assertion for the phpPoA and also acts as a SAML SP for the IdP to send the attributes to.

The communications that happen between these modules (OSID, PAPI GpoA and SSP IdP) for the initial authentication process can be seen, in a simplified form, in figure 2.

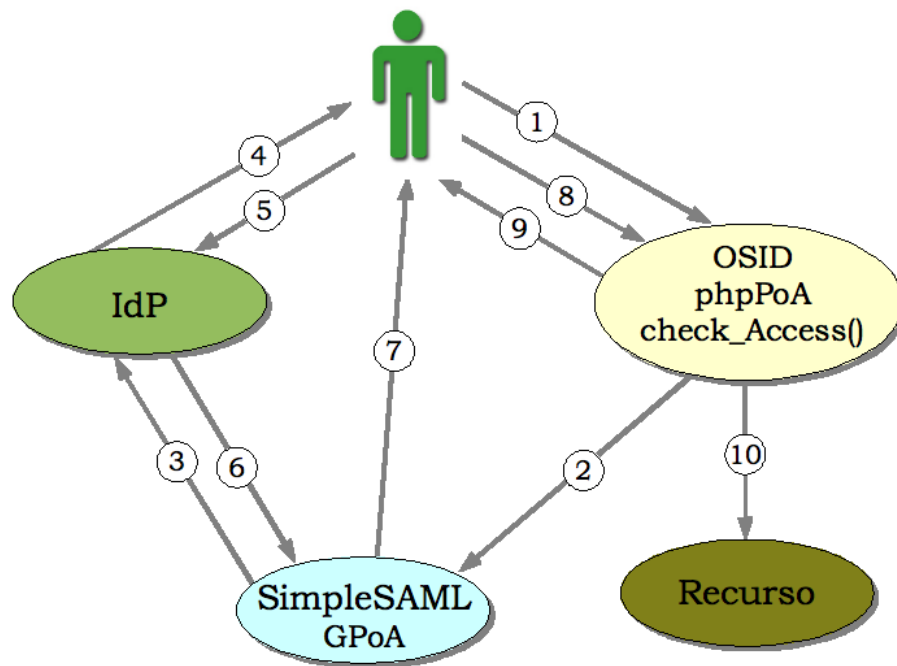


Figure 2. Authentication process using OSID, PAPI and SimpleSAMLphp

1. The user tries to access a protected area in the application, the request is intercepted by the authentication OSID that call phpPoA to check the user authentication.
2. phpPoA redirects SimpleSAMLGPoA for a PAPI assertion
3. SimpleSAMLGPoA redirects to SimpleSAML IdP for user authentication
4. The IdP presents the user the login form.
5. The user fills in the data
6. The Idp validates the data and sends attributes back to SimpleSAMLGPoA
7. SimpleSAMLGPoA builds a valid assertion and redirects the user back to the requested resource
8. The user accesses the resource again
9. phpPoA sends a cookie to the user
10. phpPoA allows access to the requested resource

Although it may seem complex, the whole process is transparent to the user, who only gets the login form - managed by the IdP and, thus, decoupled from the application - and, once validated, the requested resource. Subsequent requests will be authenticated thanks to the cookie, as usual in PAPI environments, and then by the SimpleSAMLphp session.

This approach makes easy to integrate external applications such as Dokuwiki (fig. 3), because both the application and the Ágora Virtual® framework share a common identity management.

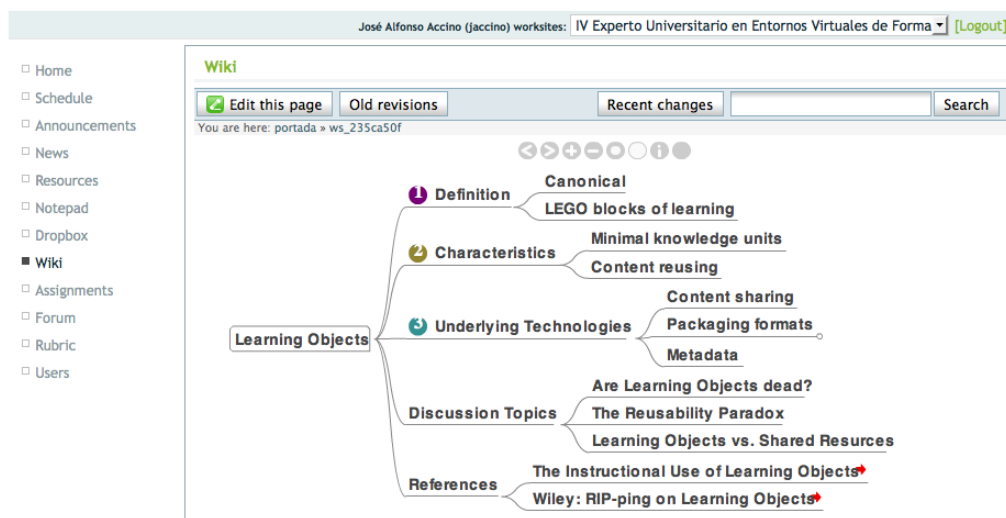


Figure 3. Dokuwiki tool integrated in Ágora Virtual@

6. FURTHER STEPS: THE CENTRAL ICT APPLICATION CLUSTER

The University of Málaga Central ICT systems team has applied this concepts the design what we have called an identity based application cluster for supporting research groups, that might be later extended to the whole community. The application cluster is no more, and no less, than several applications that can use a user common identity and enterprise information back end, by the use of IAM and, to some extent, OKI OSIDs.

The use of federation technology allows for an easy integration of members from inside and outside our University. The applications have been modified to be user origin agnostic. i.e. the user information is retrieved form the assertions sent by the Identity Providers.

This has allowed us to select the most adequate tool for a given task, such as wikis, blogs, etcetera, and even the ability to offer more than one tool, like Dokuwiki or MediaWiki, for the wiki part. The user experience results in a seamless move from one application to the other as the login information is carried over the federation protocol.

The combination of PAPI and SAML has increased the flexibility, as PAPI allows for the integration of applications where there are no SAML libraries available, such as applications developed in house for running on OpenVMS, for which a native PAPI PoA was developed some time ago.

We have also developed an special authentication and authorisation middleware for the Django web framework, that connects to the SAML federation thanks to the out of band attribute passing mechanisms of SimpleSAMLphp.

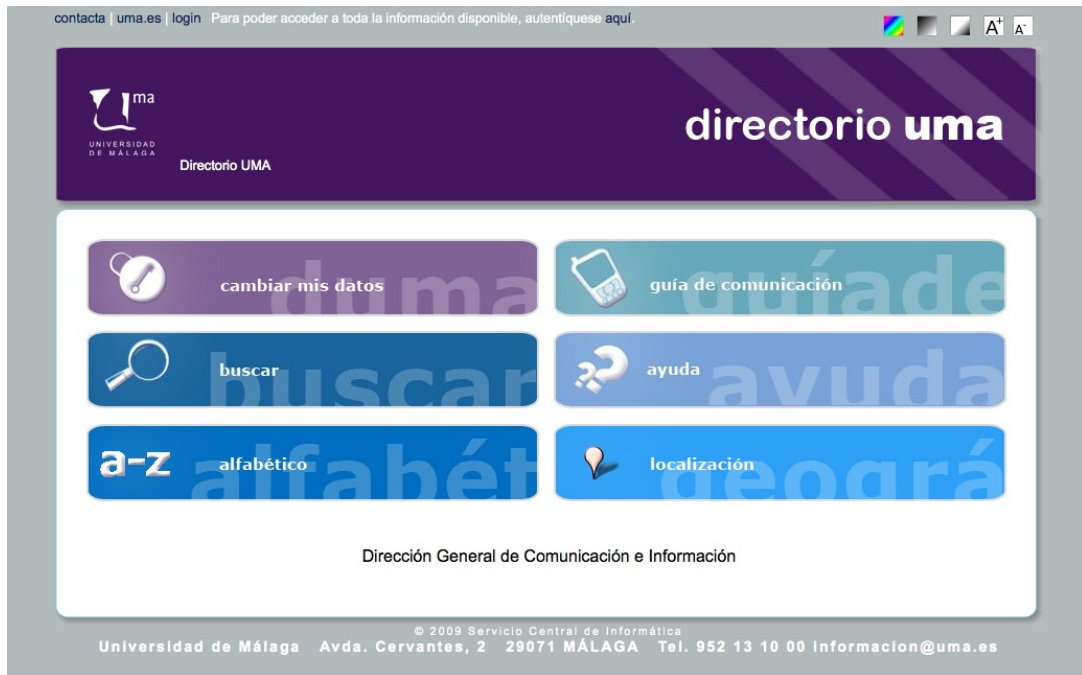


Figure 4. Directory management application built using the federated Django framework.

It should be pointed out that the road has not been free of problems as some applications have been more hesitant than others to the federation enabling modifications. This has resulted in a delay of the initial deployment of the cluster.

7. FUTURE DEVELOPMENTS

We have plans for furthering the development of this idea:

- Increasing the number of applications that can be incorporated into the cluster. We expect Django to play an important role in this.
- External authorization, decoupling an application from the decision to allow or deny access to the whole of it or some of its parts.
- This is related to group management and in this respect we are contemplating either group arithmetics or some kind of RDF graphs. We have already set some foundations for this with an initial work based on user entitlements.
- Collaboration management, transforming the concept of Virtual Environments into what Michael Gettes (now at MIT) called Collaborating Organizations: loosely coupled groups of people that gather over *the Net*, thanks to applications that share a common IAM federated infrastructure.

8. CONCLUSIONS

User centric learning, if it is to be really innovative, should be oriented towards a more holistic view of the user experience and, to this respect, daily network use is becoming more and more relevant. Thus, next generation applications, much more so learning environments, should interoperate inside the new framework where the real platform is the network and that is centered around the user.

Collaborative - groupware type - applications are not enough for achieving the above objectives, they must be made to collaborate among themselves, in the way they show and share their resources, starting with the user identity. Adapting learning environments development to this new context requires a two pronged approach: identity management and derivatives (SSO, federations)

and application interoperability standards like OKI-OSID, as a basic foundation for developing user centric environments.

The use of federated identity and standard interfaces that allow access to corporate data have proven as a corner stone for developing a new generation of applications that:

- Collaborate among themselves
- Are centred around the user
- Reduce the burden on the user: single authentication point and set of credentials
- Integrate corporate data into the learning environment
- Take the user experience outside the learning environment into account
- Use best of breed applications for each service
- Reduce the barrier to entry thanks to easier deployment

9. REFERENCES

Accino, J.A. (2006). *ÁGORA VIRTUAL: Una propuesta de entorno colaborativo y de enseñanza sobre interfaces OSID*. Retrieved May 24th, 2009 from <http://www.rediris.es/rediris/boletin/76/enfoque1.pdf>

Campus Project (2009). Retrieved May 24th 2009 from <http://www.campusproject.org/>

Cebrián, M., Accino, J.A., Raposo, M. (2007). Formative evaluation tools within ESHE: e-Portfolio and e-Rubric. EUNIS Conference. Grenoble, 2007. Retrieved May 24th, 2009 from <http://www.eunis.org/events/congresses/eunis2007/CD/pdf/papers/p85.pdf>

Coppeto, T. (2007). Introduction To OSID V3 (for developers). Retrieved May 24th, 2009 from <http://plectrudis.mit.edu/okicomunity/filemgmt/visit.php?lid=89>

Gettes, M. (2007). CO-Manage, a Collaborative Organisation Identity Management Service. TERENA EuroCAMP. Dubrovnik. 2007. Retrieved May 24th from <http://www.terena.org/activities/eurocamp/november07/slides/gettes-co11.pdf>

González, D., Palacios, J. (2005). phpPoA. Método simple de autorización mediante PAPI. *Boletín de RedIRIS*, 74-75. Retrieved May 24th, 2009 from <http://www.rediris.es/rediris/boletin/74-75/ponencia11.pdf>

PAPI documentation (2009) Retrieved May 24th from <http://papi.rediris.es/documents.html>