# Federated authentication and authorization for reusable learning objects

Luis Bellido, Víctor Villagrá, Verónica Mateos
Department of Telematics Engineering
Technical University of Madrid (UPM)
MADRID, SPAIN
{lbellido,villagra,vmateos}@dit.upm.es

*Abstract*— **The LiLa (Library of Labs) project goal is to combine virtual laboratories and remote experiments spread out over Europe, which will be shared and exchanged among educational institutions in the form of reusable learning objects. This work addresses the needs of authentication and authorization when reusable learning objects are exported from an *experiment provider* organization to *an experiment user* Learning Management System. The paper discusses possible solutions based on using the SCORM run-time environment specification as a framework for learning objects and Shibboleth as a framework for a federated authentication and authorization.**

***Keywords-virtual laboratories; remote experiments; authentication; authorization; learning objects***

## I. INTRODUCTION

The objective of the Lila project is to combine virtual laboratories and remote experiments (i.e. simulated experiments and experiments which are controlled remotely by computers) spread out over Europe, making them reachable in an environment with central retrieval and access facilitating synchronous collaboration and user generated production. The goal of this project is not only to integrate experiments and laboratories into a software infrastructure, but also to build a virtual portal in which experiments and laboratories are provided, including an on-line course system which guides users through experiments.

From the technical point of view, the LiLa portal is a repository of virtual laboratories and remote experiments on a central server, which will make it possible to include meta-data in laboratories and experiments to integrate them in library search engines and link-resolver technology. Basically, this means that virtual laboratories and remote experiments become learning objects, including learning object metadata as defined in [1]. A LiLa Learning Object (LLO) is then defined as a learning object with functionality and data elements which are specific to the access and use of virtual laboratories and remote experiments. The Lila portal gives access to these LLOs in an integrated environment, which includes a tutoring system for students and access to the 3D-engine Wonderland as a collaboration environment for students, teachers and researchers, providing users an organizational framework for online collaboration, for the transfer of virtual laboratories and connected support-services as well as for access opportunities to remote experiments.

This work was partly funded by the eContentPlus EU project ECP-2008-EDU-428037 'LiLa' (Library of Labs: Dissemination of Remote and Virtual Laboratories for Natural Sciences and Engineering).

In order to adequately exploit these learning resources, one of the objectives of the Lila project is to provide a well defined access control to laboratories and experiments. This work addresses the needs of authentication and authorization when reusable learning objects are exported from an *experiment provider*, that is, an experiment repository or a LMS (Learning Management System) of an institution providing access to resources for virtual laboratories or remote experiments, to an *experiment user* LMS, that is, the LMS of an institution which includes the learning objects as part of the curriculum for its students. In this context, the LiLa portal will act as a platform that will integrate different modules for laboratory and experiment searching, scheduling, authentication and authorization, and LLO importing and exporting. This paper discusses possible solutions based on the use of the SCORM [2] run-time environment specification as a framework for learning objects and Shibboleth [3] as a framework for a federated authentication and authorization.

## II. TECHNOLOGY OVERVIEW

### A. SCORM technology

Sharable Content Object Reference Model (SCORM) is a set of technical standards, specifications and guidelines designed to meet the functional requirements of the Advanced Distributed Learning (ADL) initiative. These standards are aimed at e-learning products like LMSs. SCORM is exclusively a technical standard, not pedagogical.

SCORM specifies that content should be packaged in a ZIP file and described in a XML file, named imsmanifest.xml (the "manifest file"). The XML file contains all the information the LMS needs to deliver the content, like information about how to launch each SCORM learning object (SCO) and, optionally, metadata that describes the course and its parts.

In LiLa, a LiLa Learning Object (LLO) is a SCO with additional constraints extended by additional metadata. Specifically, LLOs should obey the SCORM standard for learning objects, and are packaged in ZIP containers similar to regular SCOs. A LLOs is specific for one experiment or virtual laboratory, so a LLO will render a single web page, i.e, it will be a single (not composed) SCO with only a single href (html-file). Since most of the existing laboratories and experiments

use applets, a typical LLO will embed an applet providing access to the virtual laboratory or the remote experiment.

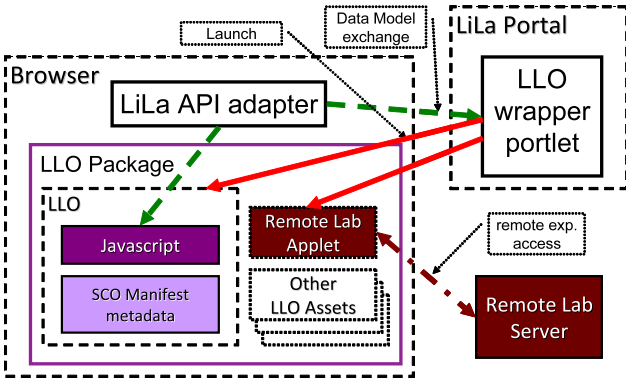


Figure 1. LiLa learning Object components

Fig. 1 shows the internal components of an LLO and the relations between an LLO, the LiLa Portal and a remote laboratory.

The LiLa portal will be based on portlet technology [4, 5], to take advantage of available functionalities such as collaboration, content management, groupware management, etc. On the other hand, there are no available portlets to display SCORM content. Having LLOs based on SCORM is important, because then it will be possible to deploy LLOs in all SCORM compliant LMSs. In LiLa a LLO wrapper portlet will be implemented to render the content that is uploaded to the portal as LLOs. This LLO wrapper portlet will be in charge of launching the LLO html page in the user browser, providing the adequate SCORM runtime environment – simplified, through the LiLa API adapter and of providing and launching the Remote Laboratory Applet, that in the case of remote experiments will have a client/server relationship with a remote Laboratory Server.

### B. *Shibboleth*

The Shibboleth System is a standards-based, open source software package for web single sign-on across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

Shibboleth allows the deployment of a federated identity management system, in which the components of the identity management system are distributed across organizations, with each organization trusting the other to perform the functions of the components they host. There are two roles in this kind of systems: organizations providing identities, that would like to provide applications only the information required to make authorization decisions, and organizations providing applications or services, that would like to manage only the identity information required for their applications, reducing the risk of storing or accidentally releasing sensitive information they do not need.

The functional components of a Shibboleth implementation support these two roles. There is an identity provider (IdP) component, which has been implemented as a J2EE component, and a service provider (SP) that has been implemented as a C++ Apache module. There is also an optional "Where are you from?" (WAYF) service, that allows to redirect users to the right IdP.

The LiLa project has selected Shibboleth as the authentication and authorization technology for the virtual portal, due among other reasons to the wide deployment of Shibboleth in educational organizations in Europe. This will facilitate the creation of a federated identity management system comprising the organizations providing virtual laboratories and remote experiments and the LiLa project as the organization that will provide a repository for experiments and laboratories, enhancing their use by including services based on the inclusion of metadata (search and catalog creation), a tutoring system for students, and collaboration services including access to the 3D-engine Wonderland.

## III. AUTHENTICATION AND AUTHORIZATION

### A. *LiLa Authentication and Authorization Architecture*

Shibboleth is the authentication and authorization technology used in LiLa to control the access by registered users to the portal as well as to control the access to experiments and remote laboratories, contained in LLOs.

As regards authentication and access control, the general portal software architecture is shown in Fig. 2.

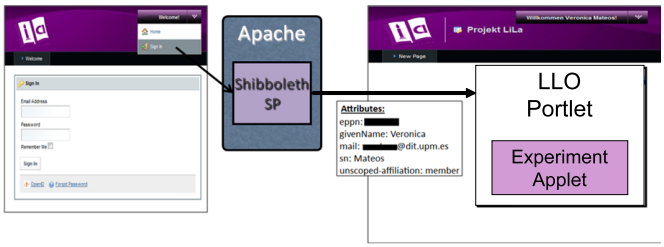


Figure 2. Shibboleth Authentication in the LiLa Portal

The general process is the following:

- A user goes to the home page of LiLa Portal. In this page the user can see some portlets.
- To access the LMS and experiments, the user has to log in the portal and go to LiLa Project page. Sign in functionality allows user to log in.
- User authentication is done using Shibboleth. As a result of the authentication process, the Shibboleth's Service Provider (SP) obtains a set of session attributes. These attributes are used to allow or deny user to access to protected resources. Also, the attributes could include information for authentication and authorization related to the LLOs which are rendered by using a portlet.
- If a user is shibboleth authenticated and she has the required permissions, she will go to the LiLa Project page, where she will see the portlets giving access to experiments and will be able to access them.

### B. *Learning Object Authentication and Authorization*

The LiLa Portal is able to check the schedule and user permissions for experiments that are contained in a LLO as far as the LLO is launched in the LiLa Portal itself. However, downloading LLOs to a LMS would bypass the portal mechanism used to check the availability of a reservation for an experiment by a user. This section discusses the authentication and authorization mechanisms used in LiLa and possible solutions to overcome this problem.

The LiLa Portal uses Shibboleth for authentication and authorization, which for the purpose of the following description means that the portal will need to have a Shibboleth Service Provider installed, which will be in charge of redirecting the requests for AA to a Shibboleth Identity Provider, that can be located elsewhere.

One possible solution to "export" the LiLa authorization and scheduling infrastructure of experiments to other systems is to both a) integrate scheduling information and Shibboleth, and b) include some way of checking AA and scheduling information within a LLO.

Fig. 2 depicts the scenario in which Shibboleth is used to perform User Authentication and Authorization, while the authorization related to a LLO is carried out by a specific "Token based LLO Authorization Server" (TLAS).

A LLO includes some information or security token, the LLO AA Token, for example in the SCO Manifest *adlcp:datafromlms* data element. LiLa could update *adlcp:datafromlms* "on the fly", if needed, when the LLO is downloaded to be included in an external LMS. A LLO is designed to get this information before launching the Remote Laboratory Applet, by retrieving the value *cmi.launch_data*.

Once the LLO AA Token is retrieved, the LLO will contact the TLAS using the token and in return, the TLAS will provide some piece of information which is needed to start the virtual experiment / remote laboratory applet. This piece of information will be passed as a parameter to the applet when launched. In the case of a remote laboratory applet, the parameter could be the url needed to contact the remote laboratory server, which might include authorization parameters depending on the level of integration of the remote laboratory with LiLa authorization and scheduling mechanisms. In the case of a virtual experiment, in which the applet is does not need access to a server, the parameter could be some access code needed to unlock the virtual experiment. The communication between the LLO and the TLAS will be based on AJAX, using the XMLHttpRequest object.

The task of the Token based LLO Authorization Server (TLAS) will be aided by Shibboleth. This server will be accessed through an Apache httpd server and protected by a Shibboleth Service Provider. This means that the TLAS will be able to perform the LLO authorization task using the user AA data provided by Shibboleth. This will make it possible to have an authorization schema where a LLO is only authorized if the user belongs to a certain organization that has obtained the access rights to the LLO. In this schema, the AA token includes information that links the LLO and the organization.

In the case of an experiment for which previous reservations are required, the TLAS could also be linked to the LiLa scheduling infrastructure, in order to only give access to the applet in case there is a valid reservation for the user. This would benefit remote laboratories that could use the LiLa reservation system even when the LLOs are used in external LMSs.

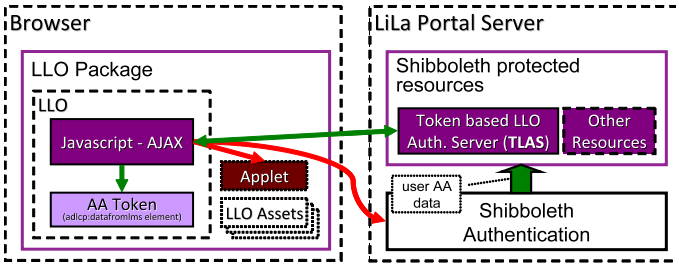


Figure 3. Authentication and Authorization for LiLa Learning Objects

Other alternatives have been considered. For example, AA attributes and scheduling information could be provided exclusively through Shibboleth. However, this would mean that in order to take advantage of remote laboratory reservations, external LMS would need to include a Shibboleth Service Provider.

Another alternative is to include the functions to check AA and scheduling status in the *LMSInitialize()* function that will be provided by the LiLa API Adapter in the LLO wrapper portlet. In this case, a LLO does not need to include any specific javascript code to perform the authentication and authorization, but when it is used in external SCORM compliant LMSs systems, no AA status check would be made unless the LMS own *LMSInitialize()* function is also modified. This could be an interesting alternative, since some of the most popular LMS are open source and LiLa could integrate the LLO AA and scheduling mechanism in LMSs such as ILIAS or Moodle.

## IV. CONCLUSIONS

The paper discusses a solution for the authentication and authorization needs of learning objects used to access virtual laboratories and remote experiments in the context of the LiLa project.

The software architecture used in LiLa requires that the virtual laboratories and remote experiments are provided as LiLa Learning Objects (LLO), which are an special SCORM encapsulation including access control functionality for interacting with the Virtual Portal authentication components in order to force that the experiments are only executed by the adequate authorized students. The objective is to enforce access control to the experiments provided by LLOs not only when LLOs are deployed on the Virtual portal, but also when they are deployed on external LMSs, taking advantage of the functionalities offered by the Shibboleth system, that allows to build a federated authentication and authorization infrastructure for web applications.

The authors are currently working on implementation of the whole system that will help confirm the viability and expose possible problems of the proposed solution.

## REFERENCES


[1] IMS Meta-data Best Practice Guide for IEEE 1484.12.1-2002 Standard for Learning Object Metadata. http://www.imsglobal.org/metadata/mdv1p3pd/imsmd_bestv1p3pd.html

[2] Advanced Distributed Learning Initiative, Sharable Content Object Reference Model (SCORM) Version 1.2. The SCORM Content Aggregation Model. 2001. http://www.adlnet.org

[3] Shibboleth, A Project of the Internet2 Middleware Initiative. http://shibboleth.internet2.edu/

[4] Alejandro Abdelnur, Stefan Hepper. JSR 168: Portlet Specification, Java Community Process. 2003. http://jcp.org/jsr/detail/168.jsp

[5] Hepper, Stefan. JSR 286: Portlet Specification 2.0. Java Community Process. 2008. http://jcp.org/jsr/detail/286.jsp