The 11th International Scientific Conference
eLearning and Software for Education
Bucharest, April 23-24, 2015
10.12753/2066-026X-15-000

ACCESS CONTROL TO THE RESOURCES OF AN OPEN DISTRIBUTED EUROPEAN VIRTUAL CAMPUS PLATFORM

Alexandru Grădinaru, Florica Moldoveanu
University POLITEHNICA of Bucharest, Splaiul Independentei 313, Bucharest, Romania
Alex.Gradinaru@cs.pub.ro; Florica.Moldoveanu@cs.pub.ro

Alexandru Soceanu, Gudrun Socher
Munich University of Applied Sciences, Lothstr. 64, 80355 Munich, Germany
Soceanu@cs.hm.edu; Gudrun.Socher@cs.hm.edu

Alberto Eloy Garcia Gutierrez
University of Cantabria, Avenida delos Castros S/N, 39005 Santander, Spain
Alberto.Garcia@unican.es

***Abstract**: The increasing number of cyber-attacks has become a global problem for companies, public institutions, even for governments and for each particular user. Cybercrime causes damage of about 750 billion EUR every year in Europe alone. Thus, ICT security is nowadays a major concern, increasing the demand for specialists in this domain. Currently, universities do not produce enough graduates with strong network security skills able to defend against complex cyber-attacks. Recently new EU approved ERASMUS+ project (DECAMP) addresses innovatively this educational aspect. DECAMP brings together within a framework of an international partnership 6 EU universities and 3 associated partners. The project is set up to create 6 online courses with integrated heterogeneous virtual hands-on lab environments covering ICT Security issues of various application areas. Each partner creates a course corresponding to its expertise. These courses can be accessed by all the students, professors and researchers of the universities within the DECAMP consortium as well as from other EU universities. The core of the DECAMP project is an online distributed virtual campus. The paper describes the procedure developed for controlling a secure access of various types of users to the platform of eLearning course materials. The solution complies on one hand with all the differences of enrollment procedures installed at each particular EU University to verify the type of user (student, teacher, researcher, etc.) requiring access to the institution's resources. On the other hand the developed mechanism allows the users to obtain a single sign on (SSO) account which supports their accesses to all distributed modules of the platform, placed at the corresponding universities which create and maintain them. A prototype system that has been deployed for testing the proposed solutions is also presented.*

***Keywords:** Access control, Single Sign-On, Distributed Virtual Campus.*

I. INTRODUCTION

The increasing number of cyber attacks has become a global problem for companies, public institutions, even for governments and for each particular user. Cyber crime causes damage of about 750 billion EUR every year in Europe alone. Thus, security in Information and Communication Technology (ICT) is nowadays a major concern, increasing the demand for specialists in this domain.

Currently, universities do not produce enough graduates with strong network security skills able to defend against complex cyber attacks. DECAMP (Open Distributed European virtual Campus on ICT Security), the new EU approved ERASMUS+ project, addresses innovatively this educational aspect [1]. DECAMP brings together, within a frame of an international partnership, 6 EU Universities

(Munich University of Applied Sciences, Germany (MUAS); University POLITEHNICA of Bucharest, Romania (UPB); University of South Wales, UK (USW); Helsinki Metropolia University of Applied Sciences (MET); University of Padua, Italy (UNIPD)) and 3 associated partners (Siemens AG, Germany; Info World, Romania and Aix-Marseille University, France).

This Erasmus+ strategic partnership project is set up to create courses which cover theoretically and practically the ICT Security issues of various areas of following applications: Network management and computer networks (MUAS), eHealth systems (UPB), Wireless networking (UNIPD), Applied forensics (USW), WEB application (MET), Cloud networking (UC).

Each partner creates a course corresponding to its expertise. These courses can be accessed by all the students, professors and researchers of the universities within the DECAMP consortium. In this way, the partners complement each other in order to cover courses on multiple topics regarding major security problems of ICT based applications. In addition, it is planned that also non-credit students of the partners or students and teachers of other EU Universities should receive access to the materials of the DECAMP campus. Consequently, one of the complex issues to be solved is a secured access control of various users to the network of interconnected eLearning modules of the distributed eLearning platform. This project will create a new experience of collaborative eLearning, which can be exploited in case of some other eLearning projects as i.e. the one described in [8].

The paper describes the proposed mechanism to implement the access control of various users to the distributed DECAMP platform. The system allows users to obtain a single sign on (SSO) account that supports their access to all distributed modules of the platform. A prototype system which has been deployed for simulating and testing the several algorithms of the proposed solution is also presented.

II. RELATED WORK

The DECAMP project pioneers the creation and implementation of a new model for an open technology campus. Relevant publications show that the e-learning is heavily on the rise [9][10][11] [12][13]. They present the experience in introducing online teaching elements based on virtual labs using virtual servers. These teaching components are available only to students enrolled at the local university. They can read some materials but don't receive any ECTS-credits. The lectures are not combined with other pedagogical elements such as instructor-evaluated hands-on lab assignments or hands-on collaborative projects. Some excerpt from the course concepts based on our experience with other online courses can be found here [14] (figure 1).

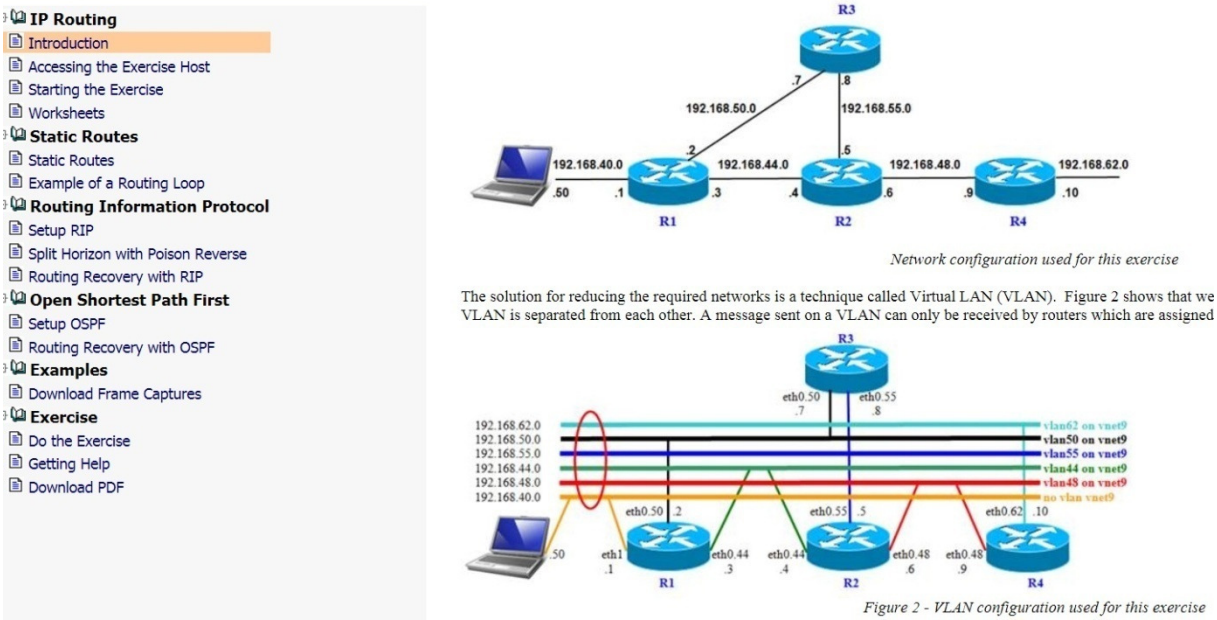

Figure 1. Carry out an experiment in the Virtual Lab

DECAMP compared with other forms of online education, e.g.:

- The FTA Academy, set up with EC support 2008-2010, merely offers courses on demand [15].
- The UK-based Open University, claiming to be "the world's leading provider of flexible, high quality online degrees and distance learning" offers for substantial fees either a complete course set for getting a degree on IT or stand-alone courses but not on network security nor lab-based education [16].
- The Virtual Labs [17] have more than ten participating Indian universities, offering virtual labs (not network security labs), free of charge. Unlike our approach, they limit themselves to a national scale and cannot offer credits for European students.
- MOOC [18] does not accept technology courses for credits. The reason: They do not have labs, have no possibility to check the students' projects and cannot carry out exam face-to-face [19].
- Coursera [20] neither offers courses on ICT security nor on computer networks.
- e-Labs are mainly offered for non-technology subjects and only for own students. They are not part of credit courses [21] and the usage of such labs is neither advised nor assessed.

III. SYSTEM ARCHITECTURE

The core of the DECAMP project is an online distributed virtual campus platform. The courses integrate heterogeneous virtual lab environments with hands-on remote applications.
The architecture of the DECAMP distributed platform (figure 2) consists of:

- Course User Admission and Information System (CUAS) - the authentication and registration system of EU students and teaching staff,
- University Virtual Learning Platform (UVLP), located at each partner, containing course materials and link to the Virtual Lab Platforms (VLP),
- VLP and Virtual Real Equipment Platform, located at each partner - the software and hardware support of all types of remote labs offered in the courses.

The secured access control of various type of users from the different DECAMP partners as well as from other EU universities to the eLearning course materials, virtual and real labs has to be implemented. The system has to comply with all the differences of enrolment procedures installed at different EU universities, to verify the type of user (student, teacher, researcher, etc.) requiring access to the institution's resources. On the other hand, the solution has to consider that the course materials and the labs are distributed on the virtual campus and placed at the institution which creates and maintains them.

IV. ENROLLMENT AND AUTHENTICATION SOLUTION

The first step in the DECAMP deployment is to design, implement and test the CUAS module. Some existing solutions presented in the literature were analyzed [6], [7]. The main problem in case of DECAMP is the difference in the enrollment and authentication procedures of the users. Each partner university has a customized local solution of registration and verifying the access to their local resources of their own users. For the DECAMP platform, two types of solutions and technologies are possible: a central and/or a distributed solution. The solution presented in this paper is based on a distributed access control to the distributed resources of the platform, which involves implicitly all local types of access control already existent at the partners. Taking into consideration that all the partner universities use Moodle as their main UVLP, the distributed solution will be based on the use of Moodle plug-ins. It supports the authentication and the course enrollment procedures local at each partner university according to their own already implemented rules (i.e.: Shibboleth, LDAP, etc.) but it allows an optimized and secure access to the distributed platform materials and labs.

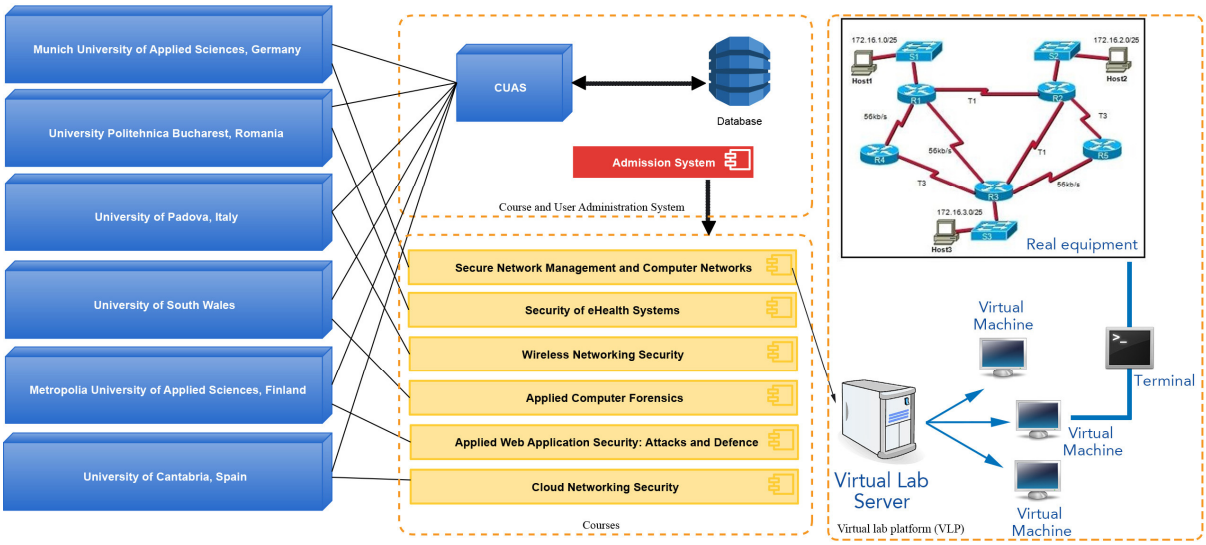

Figure 2. Architecture of Open Distributed European Virtual Campus on ICT Security (DECAMP)

3.1 Moodle Community Hub (MCH)

MCH provides a directory of courses for public use or for private communities. Only sites that are registered with the Hub are allowed to publish content there. DECAMP Community Hub (DCH) is our private MCH installed, configured and maintained at a central location at the University POLITEHNICA of Bucharest.

3.1.1. Registration of a partner and publish a course with the DCH

Each DECAMP Moodle site of the partners will have to register with the central DCH [3] in order to make public to all the users the available courses offered by the DECAMP platform. The registration is valid only if the confirmation message is displayed.

After registration, a partner can submit courses to the Hub using the "Publish" link in the course administration menus. There are two options for publishing a course: a) advertise the course for students to enroll for credits, or b) share the course for other teachers to download and install it on their own local Moodle sites [2]. DECAMP project will support both options. The teachers are encouraged to download some modules of various courses in case they need to embed these materials into their own courses. The downloaded materials may be saved as local private files or to a local Moodle server. This service is open and free of charge to any user of the DECAMP Platform.

A course can be advertised for listing using several options like name, description, category subject (e.g. Security or e-health), license (e.g. Creative Commons), tags, education level, notes and even images or screenshots. After a course has been published it must wait for the hub administration to approve it. Until approval, the courses are not displayed in the Hub and users cannot find them.

The current listing status can be checked by accessing the same "Publish" section of the course. The listing can be easily updated or removed using the above mentioned administration section Note that for each update the course must be approved again by the hub administrators.

A diagram presenting the messages exchanged by the partner Moodle sites, needed for publishing courses and listing the existing courses within the DECAMP Community Hub is depicted in figure 3.

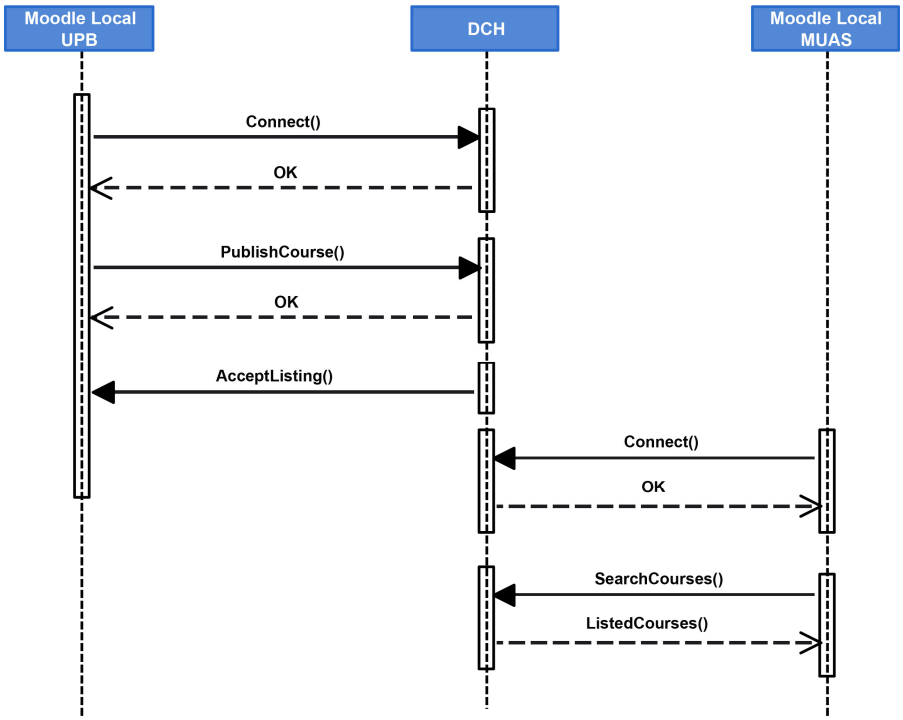

Figure 3. Publish and List the courses

3.1.2. Community Finder Block (CFB)

After all the courses are "published" to the DCH, the various users of DECAMP platform are able to find the links to the supported courses using the CFB. The CFB provides a directory of courses for public use or for private communities allowing various types of users (students, teachers, administrators) to search for courses (figure 4). Prior to enrolling or downloading materials the interested students or teachers have the opportunity to "visit the site" in order to decide if the course corresponds to their needs.

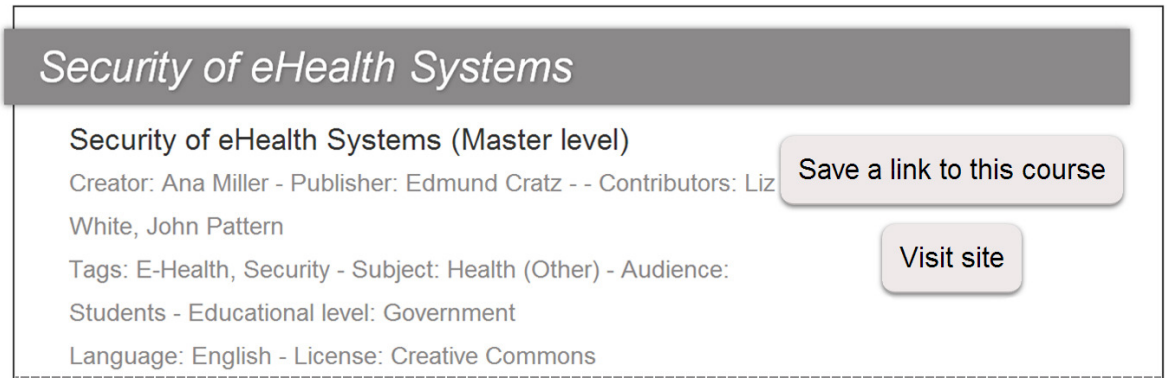

Figure 4. Community Finder Block search results

The courses may be offered for enrolling in or/and for downloading. The search result listing includes not only general information about the courses, like name, description and creator, but also details like language, subject, educational level and activities (e.g. forums, assignments etc.). The listing has also strong feedback functionality, allowing users to rate and comment on each course. The users have the possibility to save a course link in the CFB for quick access. The interested students can search the CFB and enroll for credits. This will be possible only for students who are matriculated to one of the six DECAMP partner universities.

3.2. Moodle Network (MNet)

The Moodle Community Hub does not handle the authentication of the users. In order to add authentication of type Single Sign-On (a student who take more than one course he/she authenticates only one time) the MCH module will be combined with the "Moodle Network" (MNet) administration module. This solution supports the verification of the users accessing the platform based on their local university Moodle account. Independent of the course or student locations and independent on how many courses a student intended to access, the enrollment process is executed only one time and is based only on the home university credentials. This assures the requirement of the DECAMP project that only students from the DECAMP partner universities may take courses for credit. That means, only they may use all the labs, assignments, instructor advices and only they will be able to register for exams and for getting credits.

The MNet allows a Moodle administrator to establish a link with another Moodle site and to share some resources with the users of remotely placed Moodle [4]. Users can go from the first Moodle to the linked site via the so called "Network Servers Block (NSB)". MNet is bundled with an Authentication Plug-in, which makes Single-Sign-On (SSO) between Moodle sites possible.

The Authentication protocol of MNet [5] uses tokens and sessions to provide identity to a remote user inside the network (figure 5). First, the local Moodle generates a token and a MNet session, which are sent to the remote Moodle site. This calls back the local site of the user in order to authenticate the user. The local Moodle of the user verifies the MNet session and returns the user's identity with additional data. Then, the remote site will generate an account with the received identity for the user. The users can then enroll to remote courses like she/he would be a local student using her/his home university account.

The MNet protocol is based on XML - RPC calls over an encrypted communication channel. The encryption of the messages is performed using an XMLDSIG (XML digital signature) envelope and then an XMLENC (XML encryption) envelope. To increase the security, each Moodle site is identified by its web root and also by an RSA public key.

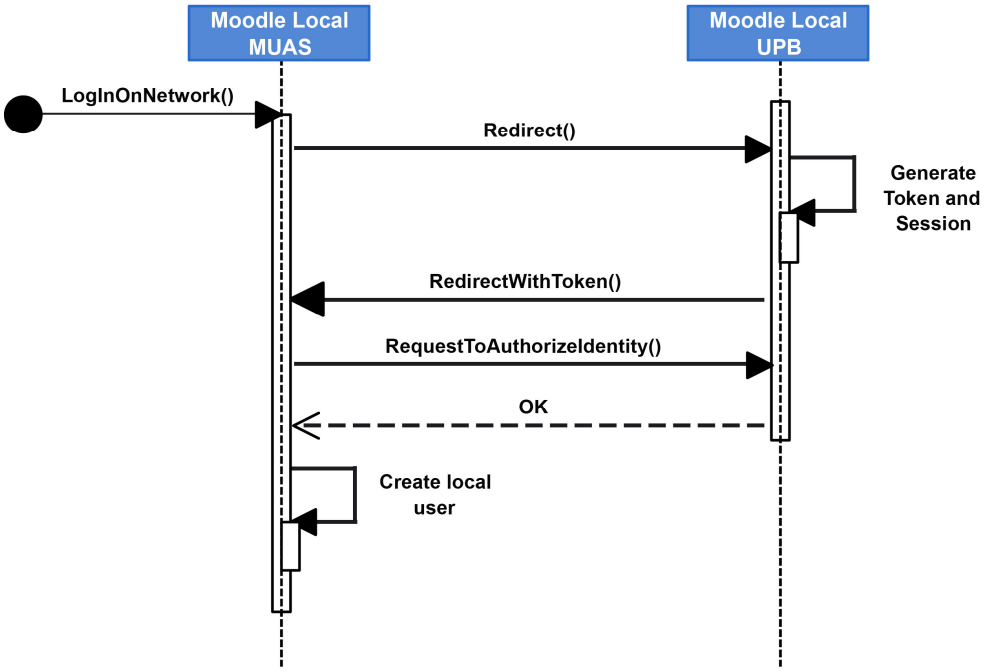

Figure 5. Authentication of a UPB student at MUAS

The encryption is made programmatically in PHP so it does not require an HTTPS server. Some PHP extensions are needed for the communication process (i.e.: Curl and OpenSSL). In order to allow each partner university to roam across the Moodle installs, the system is organized in a peer to peer network. Each partner Moodle site is connected directly to each of the other Moodle sites in the DECAMP network (figure 6).

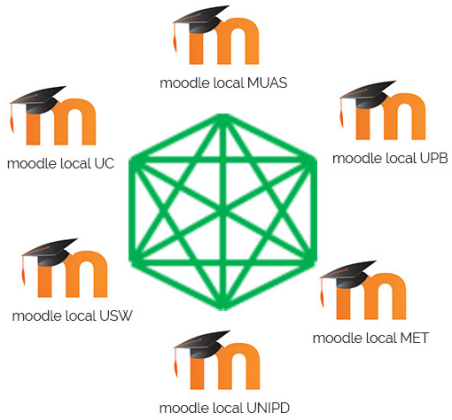

Figure 6. Peer to Peer network between the partner Moodle sites

V. SOLUTION VALIDATION

To validate the presented solution a prototype system was developed and installed. It contains a central hub called "DECAMP hub", and two separate Moodle installs: "*moodle local upb*" and "*moodle local muas*", each one with one course available and published to the hub (figure 7).

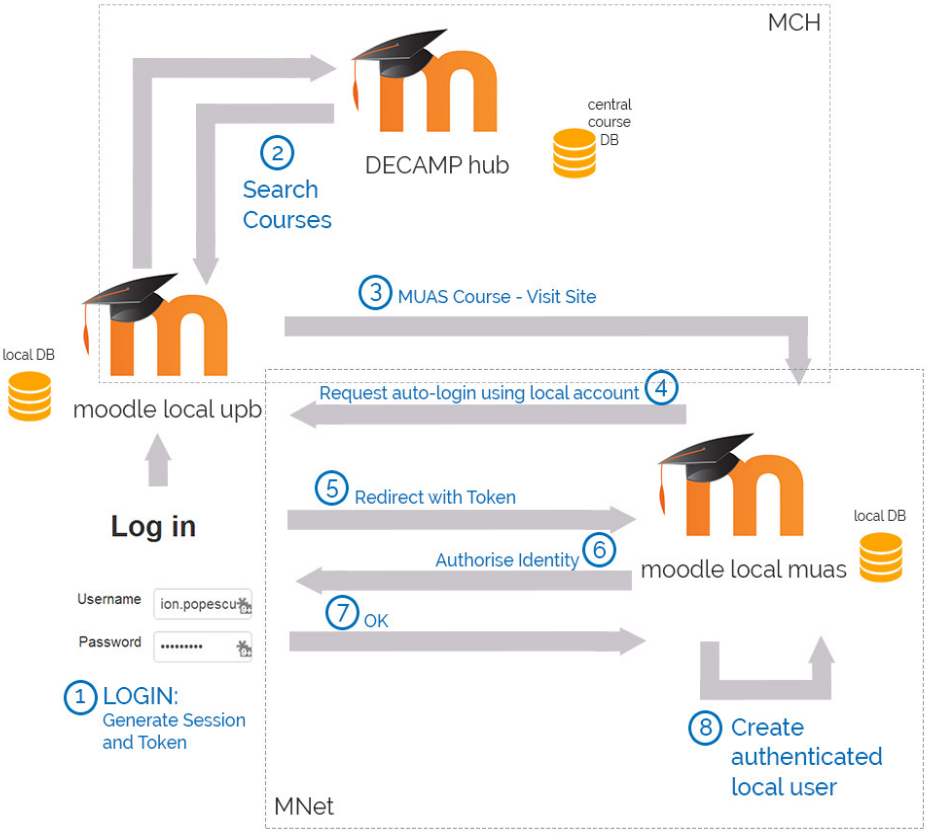

Figure 7. Simulated access control scenario, involving UPB and MUAS

Figure 7 depicts a simulated scenario: a user from UPB with the username "Popescu" logs in to his local Moodle server as usual, and clicks on a link to a course from a partner Moodle site. MNet-SSO plug-in procedure will establish a fully authenticated session for the user "*Popescu"* on the remote site. MNet module has established a fully authenticated session for the user "*Popescu*" on the remote Moodle site from Munich University.

VI. CONCLUSIONS

The presented solution for access control will be implemented for being tested first on Moodle systems of UPB, MUAS and UNIPD Project partners. Apart from this solution some centralized solutions will be also implemented and tested. The decision for the final solution will be taken considering a serious of factors like: amount of configurations needed on each Moodle system, required maintenance activities, scalability in case some more partners are added, performance, security, features supported by Moodle new versions, etc.

Acknowledgements

The DECAMP project is supported by the EU under the grant „Erasmus+ Strategic Partnerships", Agreement number 2014-1-DE01-KA203-000695.

Reference Text and Citations

[1] http://graphics.cs.pub.ro/decamp/, Accessed February 2014
[2] https://docs.moodle.org/28/en/Publishing_a_course, Accessed February 2014
[3] https://docs.moodle.org/28/en/Community_hubs, Accessed February 2014
[4] https://docs.moodle.org/28/en/MNet, Accessed February 2014
[5] https://docs.moodle.org/dev/MNet_Protocol, Accessed February 2014
[6] Moulton College: Single sign-on makes life easier for students; http://archive.excellencegateway.org.uk/page.aspx?o=291790, Accessed February 2014
[7] R. Ebner, W. Hommel, "An identity management web service for privacy-preserving course authorization in federated E-Learning", Leibniz Supercomputing Centre, Germany , EUNIS 2011; http://www.eunis.ie/presentations/whommel-elearning.pdf, Accessed February 2014
[8] MI. Dascalu, A. Moldoveanu, EA. Shudayfat, "Mixed Reality to Support New Learning Paradigms", Proc. of the 18th International Conference on System Theory, Control and Computing, Sinaia, Romania, October 17-19, 2014, pp. 698-703, ISBN 978-1-4799-4602-0
[9] J- M. M. Waldrop. "Education online: The virtual lab", Nature, Intern. Weekly Journal of Science, July 17, 2013, http://www.nature.com/news/education-online-the-virtual-lab-1.13383, checked Apr. 6, 2014
[10] Zhao and B. Forouraghi. "An Interactive and Personalized Cloud-Based Virtual learning System to Teach Computer Science". In: J.F. Wang and R. Lau (eds.), Advances in WEB-Based Learning ICWL 2013, Springer, 2013, pp. 101-110
[11] L.C. Chen et al. "Teaching Web Security using Portable Virtual Labs", 11th IEEE Conf. on, Adv. Learn. Techn., USA, 2011, 491-495
[12] C. Willems et al. "Practical Network Security Teaching in an Online Virtual Laboratory", Proc. of the 2011 Intern. Conf. on Security & Mgm., Vol. I, 65-72
[13] M. Marsella, "Technology-enhanced Learning in Europe", EC, 11th IEEE Intern. Conf. Adv. Learn. Techn., 2011
[14] "Online interactive courses for Virtual University Bavaria", http://comserver.hs-regensburg.de, Accessed February 2014
[15] http://ftacademy.org, Accessed February 2014
[16] http://www.openuniversity.edu, Accessed February 2014
[17] http://www.vlab.co.in, Accessed February 2014
[18] http://mooc.org, Accessed February 2014
[19] http://chronicle.com/article/A-Universitys-Offer-of-Credit/140131/, Accessed February 2014
[20] https://www.coursera.org/, Accessed February 2014
[21] http://www.wscc.edu/programs/student-support/elabs.htm, Accessed February 2014