Incorporating Flexible, Configurable and Scalable Security to the Education Collaborative Environments

Thiago M. Gualberto, Sergio D. Zorzo
{thiago_gualberto,zorzo}@dc.ufscar.br

Abstract - This paper presents a service that provides security through the technology of Web Services. The use of web services to provide security in e-learning systems will complement the features of services developed in language and/or different architectures. Thus, our work is not limited to platforms in which the client (e-learning system) was developed, since this service is provided on a flexible, scalable and configurable way. The proposed service uses public key cryptography, digital signature and secret key cryptography to provide integrity, non-repudiation, confidentiality and authenticity. The main features of the proposed service are presented in this paper, with their employability in a case study for the chat tool for collaborative learning environments, Sakai and Moodle. The completion of the case study is a contribution to the environments above, since the chat tool in these systems does not have security services. The case study shows the proof of concept for the security service presented in this paper.

Index Terms – Web Services, Security, Sakai and Moodle.

INTRODUCTION

Institutions of education invest significantly in the implementation of systems for e-learning. The benefits of the teaching-learning process justify the efforts of organizations to work in distance education.

The e-learning systems are used by several people. Thus, security becomes a fundamental requirement, since these systems are subject to "malicious" attack [1].

In the domain field of e-learning, the research has focused mainly in the way that learning content is provided to users of the system, without considering the security requirements in most implementations [2].

However, the security threat cannot be neglected, mainly because e-learning applications are built on heterogeneous architectures, distributed, open and can be vulnerable to ill-intentioned people. The security of e-learning role is to provide a section end-to-end secure between the student and the e-learning system [3]. Important aspects that are present in the international standard ISO and ITU-T such as data confidentiality, non-repudiation, data integrity, authentication and access control should be considered in the system.

One of the reasons why it is necessary for an e-Learning system to require security mechanisms is ensuring the privacy of the student regarding their academic performance so as to restrict access to unauthorized persons. A student may have an interest that only he and the teacher have access to their notes – access control and authentication. Ensuring that the integrity of a document or message sent by a student to the teacher is not affected, is also expected - data integrity and non-repudiation. Preventing students from frauding assessments; not allowing the services to be unavailable because of malicious attacks by third parties, and the fact that the content of learning is proprietary, are other reasons that justify the use of security mechanisms.

Confidence in e-Learning systems is a prerequisite for the acceptance of users. Thus, the use of security in electronic learning is important; since the entire system is subject to suffer new threats [4]. Therefore, we find the need to protect e-learning systems not only from fraud but also the integrity of the content itself.

Looking at the need for security in e-learning systems, the work presented in this article aims to provide security for applications in e-Learning systems.

Among the 5 types of security requirements present in international standards mentioned above, the first 3 will be treated in this work. In addition to these requirements, this work also includes authenticity.

Once observed the existence of various e-learning systems implemented on programming languages and different architectures, such as Moodle, Sakai, among others, a service that provides security through the technology of Web Services is presented in this paper [5]. The adoption of this technology is justified by the characteristics of platform-independence and heterogeneity of languages [6], which avoids the need for a security service implemented in an application that was developed in Java to be, again, implemented or restructured to be used in an application developed, as in PHP language. Thus, the proposed service can be used for e-Learning systems, regardless of language and architecture that were developed.

The remainder of this paper is organized as follows: section 2 describes studies related to this present paper; section 3 outlines the security service; section 4 describes a case study; while section 5 presents the final considerations.
RELATED WORK

Because of the information exchanged between users of collaborative learning environments and stored in it, such as notes, tests, among others, there has been the necessity of the use of security technologies to meet the need for high levels of confidentiality and privacy in e-learning systems.

However, in the following paragraphs, we present some work related to security and privacy in e-learning systems, which have some intersection with the work presented in this article, and make it possible to identify the contributions to be made.

One approach to consumer-supplier negotiation, by Yee and Korba 2007, performs the customization of security services in the environments of the Internet, and e-health, e-commerce, among others. The authors presented a new method of providing aid during the negotiation, with the intention of increasing the security services required in the environments mentioned above. Four types of security services were also added, such as logging insurance, certification, Malware Detection and Tracking Applications, in addition to the security services in international standards ISO and ITU-T [5] [8].

Another contribution of Yee and Korba's work was the creation of a prototype for the negotiation and customization of security between a consumer and supplier. This prototype was based on architecture in JADE (Java Development Framework).

In relation to Yee and Korba's work, which focused on Internet services in general, this work has, as a contribution, the offering of some security to the area of e-learning through the technology of Web Services.

The work of Webber et. al presents the implementation of a multiagent platform, which consists of a distributed infrastructure to handle security matters, which was also used for the development of e-learning environments [9].

Webber et. al identified some threats to e-learning applications, such as unauthorized access to data, unauthorized access to data during the encryption, no encryption, denial of service, absence or inadequacy of mechanisms for staff authentication, unsafe passwords, among other. These threats are related to the integrity, privacy and access control.

One of the objectives of the work presented in this article, concerning Webber's work, is to address aspects of security in e-learning environments by means of an architecture oriented to services, which are Web Services. So, the security of e-learning environments developed in different languages and architectures may be offered, due to the characteristics of Web Services, a platform of independence and diversity of languages. In order to extend the work of Webber, this paper aims to address the issues of confidentiality, non-repudiation and authenticity, and integrity provided in [9].

Raitman et. al evaluated the sense of security as experienced by students using the wiki platform as a means of collaboration in the online environment of higher education. The authors showed the importance and benefit of promoting a sense of security in an e-learning environment.

The authors in [3] analyzed the security of the Wiki platform through two mechanisms: login and anonymity. However, the work proposed here aims on implementing and evaluating security tools and services in other environments of Sakai and Moodle, such as a chat tool that was used for the case study.

Lin et. al proposed a series of applications of distance education developed in the laboratory where they work, and showed how security and privacy can be integrated in such applications. They had the privacy and security requirements together with possible solutions to remedy the requirements of each application. However, results of use of these solutions were not presented by the authors.

Considering the requirements of the PKI for online distance learning, the potential application of attribute certificates (AC's) in a proposed trust model is discussed in [11].

The application of AC's to support m-learning (mobile learning) is presented with an experimental test using a mobile device with limited resources in GPRS networks. However, the authors did not analyze the use of the proposed trust model in an e-Learning system. They have not focused on different architectures and programming languages in which the e-Learning systems can be developed and implemented. For this reason, the trust model might not fit a particular system.

INCORPORATING FLEXIBLE, CONFIGURABLE AND SCALABLE SECURITY TO THE EDUCATION COLLABORATIVE ENVIRONMENTS

The service proposed in this article provides security for applications in environments of collaborative teaching. This service complements the features in e-learning environments today.

Figure 1 shows the components that use the service and that are used by it. It is an adaptation of distributed multi-tier architectural pattern to cover the components present in the work presented in this article.

The first layer presents users (students) how to access the Internet through the collaborative learning environments from their homes, universities, or through any electronic device that has Internet access.

In the second layer, there are the Learning Management Systems (LMS), i.e., the environments for collaborative teaching. Among the existing LMS's, this article includes the following: Moodle and Sakai. These environments with their tools and services such as chat, forum, Whiteboard, sending the file, assessments, among others, are present in this layer.

The third layer contains the server application. It included a web layer in which the service proposed in this paper and the layer of business are the components (enterprise beans). In the business layer, security issues such as confidentiality, integrity, non-repudiation and authenticity
are addressed. Both layers (the web layer and business layer) run on the Java EE server.

In the fourth layer, there is the database of server application, where a Public Key Infrastructure (PKI) Key Generating and Storing Central (KGSC) are available. The PKI is a Certification Authority (CA) that is responsible for issuing and managing digital certificates used by the service. These digital certificates are stored in a repository of certificates. The KGSC has a repository of secret keys used to perform operations for symmetric encryption.

![Diagram](https://via.placeholder.com/150)

**FIGURE 1**

**COMPONENTS THAT USE THE SERVICE AND THAT ARE USED BY IT.**

### I. Service Operation

The availability of such service is performed by means of Web Services, so the service can be used for e-Learning systems regardless of platform or language in which they were developed. Thus, one of the contributions of this paper is to take advantage of the characteristics of Web Services and provide security for e-Learning systems.

A system of e-Learning, to ensure the security issues mentioned above, makes SOAP requests [12]. Specifically, these requests are made in the code of the tools and services of the e-Learning. In the SOAP request, information like: OID's (Object Identifier) of users, messages, the private key of a user, files, among others, are passed to the SOAP service on request. After receiving a request, the service features such as digital signature, encryption, signing and verification of decrypting are activated according to the tool or e-Learning system service that is using it [13] [14].

The service constantly makes requests for the PKI to verify whether the digital certificate, together with the OID of the user, is revoked or not. Through such requests to the PKI, the service can acquire the public keys of users to encrypt messages and files. The KGSC also receives requests from service so that it acquires the secret keys of users.

With the proposed service, security issues above can be offered as some tools or services of collaborative learning environments, some do not offer security requirements.

### II. Service Security

The service can be used by any e-Learning system. Thus, it is important to have the security of the service beyond the security at the time it is used by a client application. For this, we used a specification called Web Security Service [15] that extends the SOAP protocol. This extension is a way to deploy security mechanisms such as authentication, access policies and encryption for building secure web services. Thus, it has set restrictions on access to data and services, while ensuring the safety of the proposed service.

The use of this specification was made with the implementation of the library ws-security, both in the client code as in the service code. It was possible to obtain a secure connection between the client applications (e-learning systems) and service, that is, ensuring a safe end-to-end not only at the transport level as well as at the message.

### III. Service Implementation

Before the beginning of the implementation of the service, we studied many technologies suited to satisfaction of the requirements and needs of the e-Learning systems. All technologies must be distributed under a free-software license. The technologies chosen were:

- **General development platform:** Java, because it has vast available documentation, and a huge installed base of software developers and libraries.
- **Enterprise platform:** Java EE 5, because it offers a mature, integrated, well documented solution to enterprise-class software requirements.
- **Desktop development platform:** Java SE 6, based on the chosen general development platform.
- **Integrated Development Environment:** Netbeans 6, because it has advanced features related to user interface design and web service creation.
- **Database:** MySQL 5, because of its high performance, installed programmer base, and better integration with more recent versions of Java SE. Used to store the secret key in KGSC.
- **Web container and application Server:** Apache Tomcat 6. Used as the server where the service is available.
• **Object-Relational Mapping Framework:** JPA, because it is the standard Java EE 5 platform persistence framework. Persistence is the database of KGSC.

• **ws-security:** OASIS specification that provides security for Web Services.

• **Java Security:** Java API is also a provider of specifications Java Cryptography Extension (JCE) and Java Cryptography Architecture (JCA) [16] [17].

• **Bouncy Castle:** Bouncy Castle Crypto API's [18].

**CASE STUDY**

The proposal is validated by a case study in which the chat tool of collaborative learning environments, Moodle and Sakai was applied [19] [20]. The adoption of the Sakai environment is due to the fact that it is completely written in Java, and its services and tools are componentized - which allows its reuse. The fact that Sakai is directed to services was fundamental for the use of the service presented in this work. On the other hand, the adoption of Moodle is due to the fact of being written in a different language which is PHP and has virtually the same tools that Sakai has.

In order to support or supplement the learning process of students, both Moodle and Sakai offer some services and tools, such as uploading files, sending messages, ratings, release of, among others. Tools such as chat or the chat room are also provided by these environments.

The chat, most of the times, is used with the goal of providing the immediate exchange of information and interaction among learners. This is a way to ask questions, discuss and consolidate the knowledge acquired. The adoption of this tool for the study of cases occurs due to the fact that the tool is synchronous. Another reason is because there are no effective security services incorporated into this tool to ensure the protection of information exchanged between the participants or authenticity of the shares in the chat.

Figure 2 illustrates the use of the service offered by the tools of chat environments Sakai and Moodle.

In the code of the chat tool of the above environments, SOAP requests are incorporated to the service. The library also used WS-Security to ensure security in communication between the environment and service.

Initially, User A has logged in Moodle or Sakai, and enters the chat. Users of the chat have an OID and its corresponding private key. This OID is associated with the login of the user and its public key, stored in the Certification Authority (CA) managed by the PKI.

When a user writes a message to user B, a SOAP request, in the code of the chat tool, is performed to the service proposed sending a 2-upla comprising:

```xml
<msg, OID/PrivKey>
```

The first element may be a pure message, encrypted or digitally signed. The second element may be a private key or the OID of the sender or receiver of the message. Table 1 illustrates the possible combinations of 2-upla that the service can receive.

<table>
<thead>
<tr>
<th>Function of the service</th>
<th>Name</th>
<th>Element 1</th>
<th>Element 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Codification (Public Key)</td>
<td>Clear Message</td>
<td>OID Receiver</td>
</tr>
<tr>
<td>2</td>
<td>Decryption (Private Key)</td>
<td>Codified Message</td>
<td>Private Key Receiver</td>
</tr>
<tr>
<td>3</td>
<td>Digital Signature</td>
<td>Clear Message</td>
<td>Private Key Sender</td>
</tr>
<tr>
<td>4</td>
<td>Signature Verifying</td>
<td>Message Signed</td>
<td>OID Sender</td>
</tr>
<tr>
<td>5</td>
<td>Codification (Secret Key)</td>
<td>Clear Message</td>
<td>OID Receiver</td>
</tr>
<tr>
<td>6</td>
<td>Decryption (Secret Key)</td>
<td>Codified Message</td>
<td>OID Receiver</td>
</tr>
</tbody>
</table>
The service, to perform the function 1, gains access to the PKI public key associated with the OID of the recipient and then performs the encryption. Already in line 2, the service receives the encrypted message and performs the decryption by the private key of the user who received the message.

Function 3 is similar to 1, but the cryptographic operation is performed with the private key of the sender of the message. In line 4, the service makes a request to acquire the PKI public key of the sender of the message and then verifies that the signature of the message was actually performed by him/her.

To perform function 5 and 6 of the table, the service makes a request to KGSC to acquire the secret key associated with the OID of the user and performing a symmetric cryptographic operation in the message.

The proposed service offers flexible and configurable security. Flexible because the e-learning system can have security issues on a tool or in the system as a whole. It is possible, with the proposed service, to bear the system modules as chat and file transmission service using the service and the other modules (forum, Whiteboard, for example) not using the service. The functions of the service also influence in its flexibility and allow it to be configurable, because the tools that make use of the service can define which functions of the service to use as public key encryption and digital signature, encryption with secret key and digital signature, only encryption, among others.

The proposed service is also considerable scalable.

**CONCLUSION AND FUTURE WORK**

This paper presented a service that provides security for collaborative environments for teaching. This service was implemented through the technology of Web Services and APIs using Java encryption offering confidentiality, integrity, non repudiation and authentication.

Using Web Service - to provide security systems in e-Learning - complements the functionality of services and tools developed in language and / or different architectures. Thus, our work is not limited to platforms in the system of e-Learning that was developed.

Security issues – which are included in international standards ISO and ITU-T – addressed by the proposed service were also presented, as well as the use of this service in environments of collaborative teaching. The case study presented shows the proof of concept for the security service for collaborative learning environments, presented in this work.

The contribution of the service in the case study is a contribution to the teaching of collaborative environments, Moodle and Sakai, as the chat tool has no security services.

As future work, the service can be applied in other tools and services for e-Learning systems such as whiteboard, evaluations, sending the file, among others. You can also use a real PKI (eg, ICP-Brasil) for the service to provide security for legal aspects of collaborative learning environments, since digital signatures and other cryptographic operations can have legal validity when performed with digital certificates such as the ones issued by ICP-Brasil.

**ACKNOWLEDGMENT**

We would like to thank the following Brazilian agencies: CAPES for supporting Thiago de Medeiros Gualberto in his Master Program and FAPESP, which provides funding for the TIDIA-AE project, process 05/60653-1.

**REFERENCES**


**AUTHOR INFORMATION**

**Thiago de Medeiros Gualberto**, Msc Student of Federal University of São Carlos.

**Sergio Donizetti Zorzo**, PhD Professor of Federal University of São Carlos.