TEACHING X.509/PKIX BASED DIGITAL SIGNATURES WHILE ENHANCING NON-REPUDIATION OF A WEB BASED ASSESSMENT SYSTEM

Ana Isabel González-Tablas Ferreres
Computer Science Departament (STIC), Universidad Carlos III de Madrid
Avda. de la Universidad 30, 28911 Leganés (Spain)
aigonzal@inf.uc3m.es

Karel Wouters
Dept. Electrical Engineering-ESAT / COSIC, Katholieke Universiteit Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee (Belgium)
karel.wouters@esat.kuleuven.ac.be

Benjamín Ramos Álvarez
Computer Science Departament (STIC), Universidad Carlos III de Madrid
Avda. de la Universidad 30, 28911 Leganés (Spain)
benja1@inf.uc3m.es

ABSTRACT

We describe a web based assessment system whose non-repudiation security feature is based on digital signatures. The first objective of this proposal is to enhance the students' understanding of the X.509/PKIX framework and digital signatures based on it. The second purpose is to develop a security enhanced web based assessment system, focusing on non-repudiation requirements. At the same time, this non-repudiation feature is used as a way for achieving the first objective. In this paper we describe the proposed system, the prototype we have already implemented as well as the results obtained in its evaluation by the students.

KEYWORDS

Web-based assessment, digital signatures, non-repudiation, X.509/PKIX framework, innovation in security teaching.

1. INTRODUCTION

Nature of the problem. Digital signatures are one of the core technologies in the information security field. Public key digital signatures based on the X.509/PKIX framework (IETF PKIX WG) are the foundation of several main security technologies for the Internet such as SSL/TLS, Virtual Private Networks and micropayment protocols. Also, several European countries are experimenting with electronic identity cards, which allow the citizen to produce so-called qualified signatures. These signatures are legally equivalent to hand-written signatures. The understanding of this technology is crucial for students of Security on Information Technologies courses. It is also relevant for the general public, as electronic signatures have been given legal recognition recently (E.U., 1999). The concept of digital signatures is mostly taught in introductory courses. These courses cover a large set of subjects which are all relatively novel for the students, and hence difficult to grasp.

Laboratory sessions of these courses help students to practice with a great number of concepts, seen in theory, and tools that sometimes might not be directly related to them. For example, the students of one of these courses at our university practice in computer laboratories with file system integrity verification tools, firewalls, intrusion detection systems, PGP/GnuPG tools and the OpenSSL library, after several sessions devoted to cryptography exercises. Given this fact, the assessment method chosen by laboratory teachers is to perform multi-choice tests immediately after the sessions. Performing these tests via the Web and marking them automatically on the computer would offer several advantages for both students and teachers, such as quick feedback on the students' performance and efficient use of staff time.

On the other hand, security and privacy issues stand as some of the main problems of existing e-learning systems which do not fulfil all the desired requirements in these areas (Chan et al., 2003; Warren and Hutchinson, 2003). Particularly, on-line assessment has been largely debated because of the difficulties of properly authenticating the students and providing non-repudiation features to their submissions. Non-repudiation of assessment is usually provided by logs in most known e-learning systems such as WebCT or Blackboard (Chan et al., 2003). Although digital signatures are a widely used mechanism to provide non-repudiation security services (Zhou, 2001), these systems do not include this technology yet.

During last years, an increasing effort for innovating the teaching of information systems security (Yurcik and Doss, 2001) has been noticed. Teaching security by making students to practice in real or quasi-real environments sometimes implies strong security risks. Furthermore, part of the academic community disapproves these practices as they believe that this approach educates hackers instead of security defenders. Despite difficulties and criticisms, learning-by-doing in context stands as a successful educational theory and it is more and more being integrated in the teaching of information systems security (Hsu and Backhouse, 2000).

We would like to adopt this approach to enhance the teaching of the X.509/PKIX framework and digital signatures based on it. For this reason we propose in this paper a web-based assessment system that will force the students to use this technology in a real or quasi-real environment and, hopefully, this will enhance students' learning and comprehension of it. At the same time the integration of the X.509/PKIX framework in our web-based assessment system allows the enhancement of the security features of web-based assessment systems by experimenting the integration of X.509/PKIX based digital signatures for providing non-repudiation to students submissions. Our implementation can be a first step towards a fully functional plugin for existing assessment systems.

Previous work. PGP/GnuPG (PGP) can be used to digitally sign essay-type tests and send them by e-mail, but PGP is more used for informal authentication, because of the web-of-trust paradigm it uses. The authors do not know an e-learning tool that integrates X.509/PKIX based digital signatures in web-based on-line assessment. This might seem odd as these signatures are largely used in other areas such as e-government, e-commerce or even Higher Education administrations for providing authentication and non-repudiation, and there exist proprietary software that enables electronic form signing (Adobe Form Client, Entrust TruePass). Furthermore, currently several researchers propose the deployment of PKI as a solution for most of the security problems in Higher Education (Dartmouth PKI Lab, 2001; Steinmann et al., 2002; Sura and Mukkamala, 2003) and the Dartmouth PKI Lab points out explicitly the use of this technology for providing non-repudiation in assessment. But precisely the advantages offered by this framework derived from having a centralized source of trust in comparison with other trust models that support digital signatures, make it more difficult to deploy and maintain. This could be one of the reasons that discourage its full integration on e-learning environments, or at least in e-learning tools. The authors think that once Higher Education deploy PKIs for its institutions, main e-learning tools will integrate this technology also.

There exist other proposals that use cryptography for obtaining confidentiality for the answers (Lee et al., 1997) or integrity and authentication by means of hash functions (Shafarenko and Barsky, 2000), but they do not use digital signatures for providing authentication and non-repudiation to students' assessment. Most proposals use mainly strategies such as securing browsers, monitor students, mandatory initial log-on of a proctor, logs, access control from some range of IPs, assessment available during certain limited time period, shuffle choices and randomized questions to avoid students cheating beside authentication (Lister and Jerram, 2001; Pain and Le Heron, 2003; Shepherd, 2003).

Purpose and contribution of the paper. The purpose of the paper is describing the proposed solution, the prototype of the system which has already been implemented and the results of its evaluation by students.

The main contribution of this research is to innovate in the teaching of digital signatures based on the X.509/PKIX framework. The innovation consists in trying to enhance the students' understanding and learning of this technology by immersing them in a quasi-real environment where the use of digital signatures is mandatory for them. The second main contribution is that this paper may serve as a starting point for discussing and implementing technical aspects of non-repudiation in web-based assessment system.

It has to be noticed that our proposal does not intend to be used in real distance education, but in controlled or proctored environments. The higher security required for non proctored exams would need stronger authentication solutions.

2. DESCRIPTION OF THE PROPOSED WEB BASED ASSESSMENT SYSTEM WITH INTEGRATED PKI

Two main modules can be identified in the proposed system: the web based assessment system and the integrated PKI. Within the web based assessment system two main components can be distinguished: the assessment component and the database management component. The assessment component is in charge of serving students' test performance requests, and processing the subsequent submitted answered tests. The database management component is used for consulting, inserting, modifying and deleting users, subjects and tests in database. The proposed web based assessment system with integrated PKI can be described with the simplified UML use case diagram in Figure 1.

2.1. Our web based assessment system

In our system, two main types of users can be identified: teachers and students. Between the teachers we can distinguish some special teachers who are coordinators of subjects. Coordinators perform the task of system administrators: they manage users (students, teachers, coordinators) and subjects. Coordinators have responsibility on the subjects which they coordinate, implying that they have to register any additional teacher to the coordinated subjects and enroll students to their respective subjects. Coordinators and teachers registered to a subject can manage that subjects' tests and question pool, and can also consult the systems' database. Students can only perform tests and consult their grades. In the following, we describe some details of the web based assessment system.

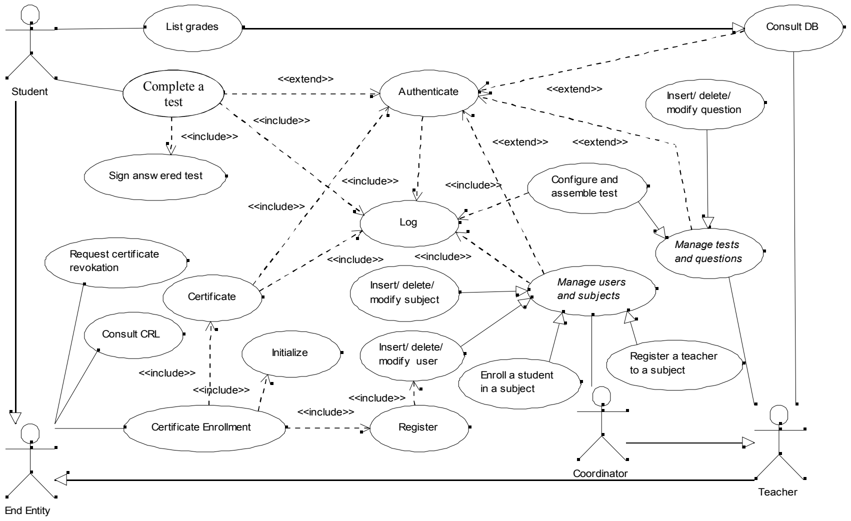

Figure 1: Use case diagram of the proposed web based assessment system with integrated PKI

Subject initialization. First, the coordinator *C* of the new subject *S* must be registered to the system as a teacher. This task might be performed by another coordinator or directly on the database. Also, some coordinator, who can be *C*, must register the new subject *S* at the same time as coordinator *C* is associated to *S*. Coordinator *C* might register at this time additional teachers to the subject or delay this task until it is necessary. Afterwards, students must be enrolled to the subject *S*, a task that might be performed automatically from a student list. If students are not registered to the system, registration must be done previously to the subject enrollment.

Question pool management and test assembling. Each subject has an associated question pool from where questions are chosen to assemble tests. Any teacher associated to a subject can add questions to its question pool, and modify and delete them if they are not used in any test. Also any teacher associated to a subject *S* can create a test for this subject, associating questions to it immediately or afterwards. Tests must also be configured before they are made available to students. This is done by associating some parameters to the test: author, an identification, access control parameters (time when it will be available, IP range from where it might be accessed) and whether bad answers result in negative scores. Questions contain the proper question, four possible answers and an indication of the correct answer. For each question a comment area is also available.

Completing a test. When a student *B* accesses the system, he/she can chose to see which tests are available and select one of them to perform it. The system sends him/her the selected test. Student *B* must answer every question choosing one of the available options and may insert a comment. When the student finishes answering, he/she must submit the answered test to the system. Before submitting it, the student must sign it. Once the test has been answered, signed and submitted, it is corrected and stored in the server, and the student receives a signed confirmation of his/her submission and the obtained grade.

Analysis of results. Both teachers and students can consult previous test grades, in the case of students, only self grades.

2.2. Providing non-repudiation to students' assessments

Our specific goal is to help students in learning the X.509/PKIX framework, digital signatures based on it and its security properties, differentiating it from other security mechanisms. Non-repudiation in a communication can be defined as a security property that provides a user with a proof about some kind of participation by another user in that communication (Zhou, 2001). In an e-learning environment, non-repudiation is a desired property in assessment works or examinations submitted by the students via the web. That is, we desire that students can not deny having submitted their assessments (non-repudiation with proof of origin), or more exactly, we desire to have a proof about the action of certain student having submitted certain assessment (preferably at some certain time) and that this proof can be verified afterwards by a third party. Furthermore, a student would like to have a proof about the reception of his/her submission by the assessment system (non-repudiation with proof of reception). Digital signatures allow the building of these proofs. Although there exist very complex non-repudiation protocols, one of the simplest ones (Zhou, 2001), which is described below, fulfills our needs:

$$1. A \rightarrow B : B, M, S_A(B, H(M))$$
$$2. B \rightarrow A : A, S_B(A, H(M))$$

Protocol 1: Non-repudiation with proof of origin and proof of reception using a hash function

where $S_X(M)$ is the digital signature of entity *X* over message *M*, and *H(M)* is the result of applying a cryptographic hash function *H* over message *M*. *A* might be a student who submits assessment work *M* and *B* the web based assessment system. Optionally, a time stamp might be included in both steps.

Using X.509/PKIX based digital signatures to provide non-repudiation properties to students' assessment influences strongly system's architecture as it forces the deployment of a PKI, which may be integrated in the system or not.

2.3. Integration of the X.509/PKIX framework in the system

In public key cryptography, each user owns a pair of mathematically related keys called the public key and the private key. For a given public key, there exists only one private key. The public key is accessible by everyone and the private key must be kept secret, and known only by the owner of the key pair. Digital signatures on a document can only be generated using the private key. These signatures are verified using the public key. Signatures that are produced this way can offer authentication, non-repudiation and integrity of the signed document.

Digital signatures must be supported by a trust model that securely binds some identification of the owner to the public key. The electronic document that ascertains the authenticity of the binding is called a digital certificate and it is usually issued by a trusted entity (Certification Authority, CA). The certificate is a digital signature by the CA, on at least the public key, the identification of its owner and a period of validity. When the private key is compromised (stolen) or lost before the corresponding certificate expires, the owner must report this to the CA to have the certificate revoked. The CA uses a publicly available list (the Certificate Revocation List, CRL) to announce certificates that have been revoked. When a signature needs to be verified, the verifier will first check the CRL of the CA that issued the certificate, corresponding to the signature. If the certificate has been revoked, the signature is considered to be invalid. Different approaches exist for trust management such as hierarchical, peer-to-peer or distributed. Each of them may configure a trust model on which the digital certificates rely. Public Key Infrastructures (PKI) specify the processes involved in the generation and management of public key pairs and digital certificates.

The X.509/PKIX framework specifies an architecture and a set of protocols conforming an X.509-based PKI for the Internet (IETF PKIX WG), and is based on the X.509 certificate format (ITU-T, 2000) and on the PKCS standards (RSA Laboratories), which define fundamental cryptographic data formats and algorithms. Nowadays, X.509/PKIX has become the standard which most of the Internet security protocols and technologies rely on.

The main components in the PKIX model are the following:

1. End entity: User of PKI certificates and/or end user system that is the subject of a certificate. In our system teachers and students are considered end entities (see Figure 1).
2. Certification Authority (CA): It issues, stores and revokes certificates. In our case, the CA is integrated in the web based assessment system.
3. Registration Authority (RA): An optional system to which a CA delegates certain management functions such as registering users. Often, the CA and RA are merged into one. The RA is not included in our system for the moment.
4. Repository: A system or collection of distributed systems that store and allow entities to access certificates and certificate revocation lists (CRLs). This component is also integrated in the web based assessment system.
5. CRL issuer: An optional system that a CA can delegate on to publish CRLs. It is not included in the system but its tasks have been assumed by the CA.

In the X.509/PKIX framework several services are specified, but we are going to deploy the basic ones which are described below and are depicted in the use case diagram in Figure 1:

End entity certificate enrollment. This use case obtains as a result the issuance of the end entity public key certificate by the CA. The process is comprised by three steps:

1. Registration; all end entities must enroll into the PKI before they can apply any of the enabled services. Usually this step is associated with the initial verification of the end entity's identity, which in our system occurs at the same time as the registration to the web based assessment system. The end entity is typically issued a shared secret that he/she must use for subsequent authentication as the enrollment process continues, and as a requirement of our web based assessment system students must deliver their digital photograph.
2. Initialization; in this step the trust relation between CA and end entity is initialized. At this point, usually, the end entity gets the CA's certificate, although this step can be postponed. The key pair associated with the end entity is generated, either locally by the user or by a trusted third party, and a certificate request is submitted to the CA. In our case, the key pair is generated locally by end entities.
3. Certification; the end entity's public key certificate is issued by CA; it is communicated to the end entity and/or published to a repository.

Certificate revocation request. An end entity may request a certificate revocation in order to make it invalid before its expiration date.

Certificate revocation list consultation. An end entity may consult which certificates have been revoked.

2.4. Additional and non functional requirements

Some other requirements can be identified in our web based assessment system with integrated PKI:

- The system should be a distributed web application and the web interface should be compatible with several browsers.
- Simplicity and usability of the system interface should be considered first over other desirable features.
- In a web based assessment system, consideration of security requirements is important (Chan et al., 2003; Shepherd, 2003). The following security properties should be provided:
  - User authentication.
  - Confidentiality of communications.
  - Access control to the system; role-based authorization for accessing different modules of the system and its features.

  - Non-repudiation of origin and reception for students assessment submissions, which has already been described.
  - Accounting (auditability and traceability) of user and system actions.
  - Integrity.
- Session security must be also provided and actions to prevent cheating should be considered.
- Key generation should be performed by the user in his/her local system and independently of the web browser. The signature process should be done by the web browser, with an external tool, that is, the process should be similar to the case of using a cryptographic smart card. This requirement also influences the architecture.

2.5. Architecture

The chosen architecture (see Figure 2) for containing our web based assessment system with integrated PKI is a two-tier servlet-based web application running on a servlet container on the server side, and a web client supported by some processing capabilities on the client side. On the server side we find also a database which contains the system's data (users, tests) and a repository with the CA's keys and certificates (issued and revoked). On the client side, JavaScript is used to perform local form validations and to improve interactivity. To achieve the requirements, the signature on the client side is performed via a signing applet which communicates with the user through java graphical interfaces and with the browser via JavaScript.

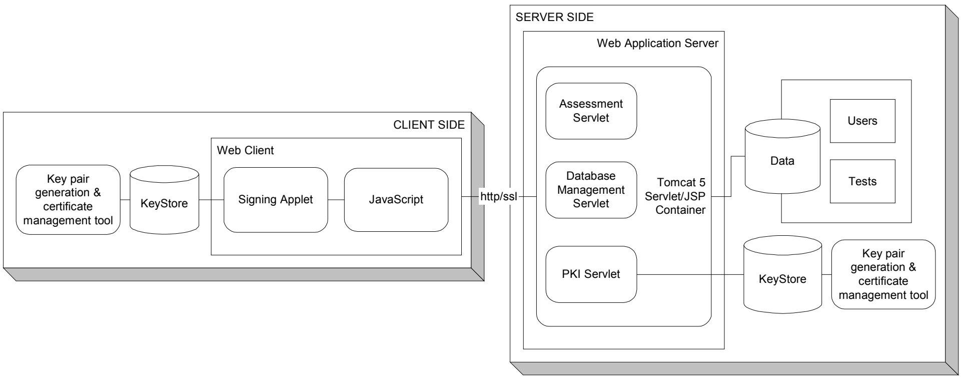
SERVER SIDE
Web Application Server
Assessment Servlet
Database Management Servlet
Tomcat 5 Servlet/JSP Container
PKI Servlet
Data
Users
Tests
KeyStore
Key pair generation & certificate management tool
CLIENT SIDE
Web Client
Key pair generation & certificate management tool
KeyStore
Signing Applet
JavaScript
http/ssl

Figure 2: Architecture of the web based assessment system with integrated PKI.

Solutions to achieve security requirements (Chan et al., 2003; Shepherd, 2003). Users authenticate with user/password, and during the test, the student's photo can be seen on the test page. To provide confidentiality, every communication with the web application server relies on the SSL protocol. Role-based authorization (teacher, coordinator, and student) is enforced in order to access web application components. Also, IP’s range and time window access control is enforced when students perform tests. Non-repudiation of students' submissions is achieved by following the described non-repudiation Protocol 1 and accounting is achieved by logging most actions. Session security is obtained using cookies and servlet context variables. Finally, to prevent cheating, exams are proctored and teachers must authenticate students checking the photo on the test page.

Signature process. Signing is performed outside the web browser, similar to a smart card signature in which the signature is generated inside the card and the private key never leaves the card. In our case, the private key will be known to the signing applet, which will perform the signature. In this step, a signed applet shows the student the answered test. Using a signed applet allows the recipient to verify the authentication and integrity of the code, furthermore, it provides a way for identifying which code is authorized with special permissions not given by default to code executed inside the Java sandbox (such as reading local files). After revising his/her answers, the student indicates where the private key is stored, and types the password that protects the key. The signing applet performs the signature, appends it to the answered test and submits it to the server.

2.6. Prototype implementation and evaluation

We have implemented a prototype of the system on a PC with Windows XP Professional (Intel(R) Pentium Processor 1500 MHz, 512 MB RAM). The used servlet container is Tomcat 5 Servlet/JSP container. Web browsers compatibility has been tested with Netscape Communicator, Internet Explorer and Mozilla FireFox.

To implement the X.509/PKIX framework, we have decided to use a Java Cryptography Provider library and the following key and certificate management tools: Sun keytool and Pankaj Kumar's Java Security Tool Kit (http://www.j2ee-security.net). The selection of this simple solution instead of other more complex PKI implementations has been made because it allows students to practise in laboratory with the same technology that they afterwards have to use in order to obtain their certificate for the web based assessment system. This facilitates the main goal of this proposal.

The prototype has been evaluated by an experimentation group of 28 volunteer students over the whole set of 83 students enrolled to the subject. Only 21 of the students in the group completed successfully the process of certification and assessment at least one of the three times they were asked to. At the end, the 28 students in the experimentation group were requested to evaluate the prototype by filling up an anonymous evaluation form. The most relevant questions contained in the evaluation form are the following:

Table 1: Questions in the evaluation form

(Figure) Serie	**Question**
(a) 1	The prototype is adequate to assess the laboratory of this subject using web-based tests
(a) 2	The prototype enhances the previous paper-based assessment process because of automatic correction
(a) 3	The prototype enhances the previous paper-based assessment process because of automatic feedback of the grade
(a) 4	It is adequate to perform ONLY web-based tests (not both paper- and web-based) using the prototype
(b) 1	It is adequate to integrate digital signature in web-based assessment systems for issuing proofs of origin for teachers
(b) 2	It is adequate to integrate digital signature in web-based assessment systems for issuing proofs of receipt for students
(b) 3	To use digital signatures integrated in web-based assessment has helped me to understand this technology
(b) 4	To use X.509 certificates and performing the related PKIX processes has helped me to understand this technology
(c) 1	Your experience in the evaluation of the prototype has been positive
(c) 2	It would be adequate to repeat the experience next year with students of this subject
(c) 3	It would be adequate to extend the experience to other subjects

Statistics obtained for these questions are presented in Figure 3. Results in Figure 3a show that students evaluate positively web-based assessment but do not completely trust it, as 46% of them do not agree on performing the tests using only the prototype (question a4). This fear is probably caused by the novelty of the system for the students or by the preliminary state of the prototype. In Figure 3b results show (questions b1 and b2) that 85% of the students agree on integrating digital signatures to provide proofs of origin and receipt respectively for teachers and students, but a slightly minor percentage of 70% (questions b3 and b4) considers that using the prototype helped him/her to understand better digital signatures and X.509/PKIX framework. Our interpretation of these results is that students assess the integration quite positively but more work needs to be done in the prototype in order to enhance its usefulness for helping students to understand target technologies. About the evaluation of their experience using the prototype, nearly 70% evaluate it positively, and consider advantageous to repeat the experience next year and in other subjects.

3. CONCLUSION

With our proposal we achieve in a simple way three goals at the same time: web based assessment, non-repudiation for students' submissions using X.509/PKIX based digital signatures, and innovating the teaching of Security on Information Technologies at Higher Education levels.

It is well known that performing Web based tests and marking them automatically offers several advantages for both students and teachers. Students' authentication and non-repudiation of their assessment submissions stands as one of the main security problems in web based learning. Although digital signatures are a widely used mechanism to provide non-repudiation security services (Zhou, 2001), most known e-learning systems do not integrate this technology yet. One of the achieved goals of the proposed system addresses this issue, as we investigate the introduction of X.509/PKIX based digital signatures for non-repudiation in multiple-choice test web-based assessments. Furthermore, another main contribution of our research is the innovation in the teaching of digital signatures based on the X.509/PKIX framework. This innovation targets the enhancement of students' understanding and learning of this technology by immersing them in an environment (the web based assessment system) where the use of X.509/PKIX based digital signatures is mandatory for them. The authors also believe that using the X.509/PKIX technology directly will motivate students to learn it.

Our web based assessment system has an integrated PKI that has to be deployed and maintained, which is not a straightforward task. Furthermore, users must be educated in the use of the PKI. This shouldn't be a problem if the users are going to be students with a computer science background, but if we want to extend the use of the system to other student profiles, we will have to make it more user-friendly and more effort has to be put in user education. On the other hand, extending the use of the system to all students offers them a relatively simple environment for understanding and learning about digital signatures in a easy way, becoming e-identity educated citizens.

Results show that the experience has been a success, although some aspects must be enhanced mainly trust of students on the system and pedagogical capabilities of the prototype.

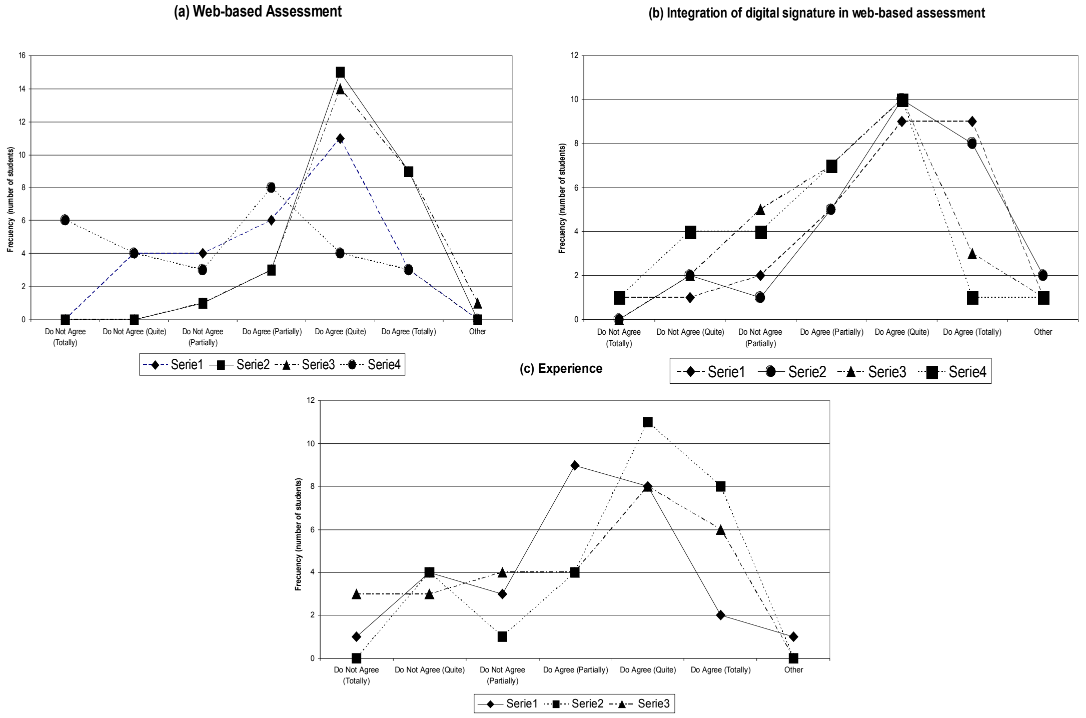

Figure 3: Statistics of the prototype evaluation by the experimentation group

Some future work can be identified:

1. Migrate the system to XML and make it compliant with existing e-learning and education standards.
2. Using the system with students from non-technical faculties.
3. Integrate the system with an enhanced out-of-the box PKI (OpenCA) with an LDAP repository (OpenLDAP) and a complete set of PKI services; integrate the system with the signature functionality on an electronic identity card.
4. Make the system modular in order to integrate it easily with other web based e-learning systems.
5. Enhance the system's functionalities, usability and security. Enhance pedagogical capabilities.

6. Explore the use of qualified electronic signatures, to ensure the legal aspect of non-repudiation.

ACKNOWLEDGEMENTS

Authors would like to thank the anonymous referees for their useful comments and suggestions, and the technical staff of the Laboratory of the Computer Science Department (Carlos III University) for their help and collaboration in the deployment and evaluation of the prototype.
The prototype has been implemented by David Sánchez Torre, student of Computer Science Technical Engineering at Carlos III University.

REFERENCES

Adobe Form Client. On-line: http://www.adobe.com/products/server/formclient/main.html

Chan, Y.-Y., Leung, C.-H., and Liu, J.K., 2003. Evaluation on Security and Privacy of Web-Based Learning Systems. *Proceedings of the 3rd IEEE International Conference on Advanced Learning Technologies (ICALT'03)*. Athens, Greece, pp. 308-309.

Dartmouth College PKI Lab, 2001. *PKI Applications in Academic Computing*. On-line: http://www.cs.dartmouth.edu/~pkilab/acapps.shtml

E.U., 1999. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. *Official Journal of the European Communities*. L 13, 1999/93/EC, pp. 12-20.

Electronic Identity. On-line: http://www.electronic-identity.org/

Entrust TruePass. On-line: http://www.entrust.com/truepass/

Hsu, C. and Backhouse, J., 2002. Information Systems Security Education: Redressing the Balance of Theory and Practice. *Journal of Information Systems Education*. Vol. 13, No. 3, pp. 211-218.

ITU-T, 2000. ITU-T Recommendation X.509: Information Technology – Open Systems Interconnection - The Directory: Authentication Framework. (Equivalent to ISO/IEC 9594-8, 2000).

Lee, K.C., Chang, K.N, Yu and C.S, 1997. Design and Implementation of Important Applications In a Java-based Multimedia Digital Classroom. *In IEEE Transactions on Consumer Electronics*, Vol. 43, No. 3, pp. 264-270.

Lister, R. and Jerram, P., 2001. Design for Web-Based On-Demand Multiple Choice Exams Using XML. *Proceedings of the IEEE International Conference on Advanced Learning Technology: Issues, Achievements and Challenges*. Madison, WI, USA, pp. 383-386.

Nash, A., Duane, W., Joseph, C., and Brink, D., 2001. *PKI: Implementing and Managing E-Security.* McGraw-Hill, California, USA.

OpenCA. On-line: http://www.openca.org

OpenLDAP. On-line: http://www.openldap.org

OpenSSL. On-line: http://www.openssl.org

Pain, D. and Le Heron, J., 2003. WebCT and Online Assessment: The best thing since SOAP?. *Educational Technology and Society.* Vol. 6, No. 2, pp. 62-71.

PGP. The International PGP Home Page. On-line: http://www.pgpi.org

PKIX IETF WG. Public Key Infrastructure (X.509) (PKIX). On-line: http://www.ietf.org/html.charters/pkix-charter.html

RSA Laboratories. The Public-Key Cryptography Standards (PKCS). On-line: http://www.rsasecurity.com/rsalabs/pkcs/index.html

Shafarenko, A. and Barsky, D., 2000. A Secure Examination System with Multi-Mode Input on the World-Wide Web. *Proceedings of the IEEE International Workshop on Advanced Learning Technology: Design and Development Issues (IWALT 2000).* Palmerston North, New Zealand, pp. 97-100.

Shepherd, E., 2003. Delivering Computerized Assessments Safely and Securely. *The e-Learning Developers' Journal*. October 20, 2003, pp. 1-9.

Steinemann, M.-A., Zimmerli, S., Jampen, T. and Braun, T., 2002. Global Architecture and Partial Prototype Implementation for Enhanced Remote Courses. *Proceedings of Computers and Advanced Technology in Education (CATE 2002)*, Cancun, Mexico, May 20-22, 2002, pp. 441-446.

Sura, P.K., and Mukkamala, R., 2003. A PKI Architecture for Academic Institutions: Design and Prototype. *Proceedings of the International Conference on Security and Management*, SAM '03, June 23 - 26, 2003, Las Vegas, Nevada, USA. Volume 1, pp. 205-212

Warren, M., and Hutchinson, W., 2003. Information Security – An E-learning Problem. *Proceedings of the Second International Conference on Advances in Web-Based Learning (ICWL 2003).* LNCS 2783. Melbourne, Australia, pp. 21-26.

Yurcik, W. and Doss, D., 2001. Different Approaches in the Teaching of Information Systems Security. *Proceedings of the 18th Annual Information Systems Education Conference – Technolgy in the 21st Century: Where Innovation and Information Converge.*Cincinnati OH. USA.

Zhou, J., 2001. *Non- repudiation in Electronic Commerce*. Artech House Publishers. Norwood, MA, USA.