A secure e-exam management system

Conference Paper · May 2006

DOI: 10.1109/ARES.2006.14 · Source: IEEE Xplore

3 authors:

Jordi Castellà-Roca
Universitat Rovira i Virgili
86 PUBLICATIONS **1,079** CITATIONS
SEE PROFILE

Jordi Herrera-Joancomartí
Autonomous University of Barcelona
115 PUBLICATIONS **1,894** CITATIONS
SEE PROFILE

Aleix Dorca Josa
University of Andorra
11 PUBLICATIONS **56** CITATIONS
SEE PROFILE

A Secure E-Exam Management System

Jordi Castellà-Roca[†],Jordi Herrera-Joancomarti[‡] and Aleix Dorca-Josa[§]
† Rovira i Virgili University of Tarragona, Dept. of Computer Engineering and Maths,
Av. Paisos Catalans, 26, E-43007 Tarragona, Catalonia
‡ Universitat Oberta de Catalunya, Av. Tibidabo 39, 08035 Barcelona
§ Universitat d'Andorra, Plaça de la Germandat, 7, AD600 Sant Julià de Lòria, Principat d'Andorra
E-mail: [†]jordi.castella@urv.net, [‡]jordiherrera@uoc.edu, [§]adorca@uda.ad

Abstract

Secure electronic exams are one of the most difficult challenges in e-learning security. The relevance of the examination process for any academic institution implies that different security mechanisms must be applied in order to preserve some security properties during different examination stages. In this paper, we present a secure e-exam management system where all exam related information is in digital format. We propose a cryptographic scheme that has to be executed in order to achieve the desired security levels at every exam stage.

Keys words: *e-learning security, electronic exams (e-exam), cryptographic protocols.*

1 Introduction

In e-learning environments, students and teachers use Internet on a regular basis in order to follow/receive lectures, ask/answer questions and send/receive assessments. However, e-learning (or in general distance learning) universities rely on an examination process in which students hold a face to face exam in a physical place determined by the university under supervised conditions. Such conditions ensure the correctness of the exam, a difficult task to achieve in a virtual exam model. Face to face exams allow to check students identity and ensure exam authoring using traditional means (checking an identity card and ensuring no one helps the student during the exam).

Ensure student identity and authoring in a virtual or distance exam has been pointed out as a hard problem in the literature [14] with a difficult solution. Then, e-learning institutions still need face to face exams. However, face to face exams represent an important effort for e-learning institutions. Typically, e-learning universities do not have enough physical facilities for all students so they have to rent buildings in order to allow students to hold their exams. Furthermore, exam management becomes more complex since such external examination centers must be provided with all management mechanism to ensure that students will be able to perform their exam in a desired location and later on, all exam answers will be properly collected and sent to the teachers that have to correct them. For all those reasons, improving exam management systems has clear advantages for distance learning institutions.

In order to simplify exam management it is desirable that all exam stages can be performed electronically, so exams are turned into e-exams. Notice that we use the term e-exams to refer to exams (in fact, all exam stages) that can be performed by electronic means. However, we do not assume that e-exams are distance or virtual exams, since such property implies different security concerns. In this paper, we assume that students hold the exam in a supervised environment, but electronically, that means the student uses a computer to take the exam.

Intrinsically, exam management needs to achieve a good security level, since the correctness of this process ensures somehow the quality of the university. For that reason, the design an electronic management system for exams should take a special care of security.

Security in e-learning environments has been addressed in different literature works. A high level overview of this topic can be found in [6, 5, 3, 14]. All these works share the main ideas regarding the way to achieve better security levels in e-learning environments. Public key infrastructures (PKI) are identified as an adequate technology in order to provide confidentiality, authenticity, integrity and non-repudiation, in e-learning environments. According to these ideas, a PKI approach for an e-learning environment has been proposed recently in [9] showing that PKI solutions deliver flexibility and scalability to an e-learning environment.

Focusing on electronic exam management, to our best

0-7695-2567-9/06 $20.00 © 2006 IEEE

knowledge, the only published work on this topic is due to Chadwick [1]. However, the project did not cover all stages of an exam detailed in [14], it only addresses the setting up stage where the examination questions are transferred between teachers using secure electronic mail based on a PKI. On the other hand, two commercial solutions for on-line examinations are available [12, 4]. However, these proposals do not describe their security measures so it is difficult to evaluate their suitability and security level.

In this paper we present a secure e-exam management system. Such system is based on different cryptographic protocols that offer a high security level for all exam stages. This scheme has been implemented in a Master Thesis [2].

The rest of the paper is organized as follows: Section 2 describes every examination stage and its security requirements. Section 3 presents our scheme for secure electronic exam management. Section 4 evaluates the security of the proposed scheme regarding the security requirements identified in Section 2. Section 5 describes the implementation of the prototype developed in the Master Thesis [2]. Finally, our conclusions are presented in Section 6.

2 Examination stages and security properties

An examination process consists of different stages. In this section we describe each examination stage and its security requirements based on our experience and on the contributions made in the literature papers [6, 5, 3, 14]. This accurate description has guided the design of a cryptographic protocol for each stage.

The examination process can be divided in the following stages:

Setting up an exam: the first stage is the preparation of the examination questions which is performed by the teacher.

Beginning, holding and submitting of the exam: in the second stage, when the exam begins, the student obtains the exam questions, she writes down the answers and finally she submits her answers. This stage must be performed within a fixed amount of time.

Grading of exams: After the student has delivered the exam, the teacher grades it.

Obtaining the score of the exam answer: Once the exam has been graded, the student obtains the result.

Revising of exams Finally, if the student does not agree with the obtained grade, she can apply for an exam revision.

Regarding the stages described above, we have identified the following security requirements, although some of them have already been pointed out in previous works [6, 5, 3, 14].

Authenticity:
- The student must be sure that the exam questions and the exam grade have been proposed by the teacher.
- The teacher must be sure that the exam answer belongs to a valid student.

Privacy:
- The exam score process should be blind in order to obtain a maximum impartiality. Then, the teacher should not know the student identity of an exam answer. However, the teacher must be convinced that the answer belongs to a valid student.

Correction:
- The exam questions can not be modified once the exam has started, that means that the integrity of the questions must be preserved.
- Once the examination time has finished, no answers can be submitted.
- Once an answer has been submitted it must not be possible to alter it.
- It should not be able to deliver more than one exam per student.
- The deletion of one exam should be avoided or at least detected.

Secrecy:
- Exam questions must be kept secret, so the exam can only be obtained by valid students during the time of the exam.
- The exam solution must be kept secret until the exam grades are published.
- The students' answers must be kept secret, only the teachers can have access to them.
- The exam grade should only be sent to the student who did the exam.

Receipt: The student must obtain a receipt as a proof that she has did and sent her exam answer.

Copy detection: The student should do the exam alone, so cheating must be avoided.

3 The proposed scheme

In this section we propose a secure scheme for electronic exam management. We rely on the fact that there is no solution to obtain the copy detection property if the students take the exam at home [6, 5, 14]. Therefore in our proposal, the exam takes place in a supervised environment.

In our proposal, we face interactions between three kinds of parties or actors, namely:

Student: We use the term *student* to refer to both a person taking part in the exam, and the software used to that end, since cryptographic operations must be performed.

Teacher: The *teacher* is the one that proposes the exam questions and grade the answers. Also in this case, we refer to both the person and the software used to that end.

Manager: The *manager* is the central authority that controls the exams. It manages the exam questions, answers, solutions and grades.

For each stage enumerated in section 2 we propose a different cryptographic protocol.

3.1 Notation

The following notation is used in order to describe the protocols presented.

- (P_{entity}, S_{entity}): Asymmetric key pair of $entity$, where P_{entity} is the public key and S_{entity} is the private key.

- $s_{entity,i} = S_{entity}(m)$: Digital signature s of message m signed by $entity$, where digital signature means computing the hash value of message m using a collision-free one-way hash function and encrypting this hash value with S_{entity}. Subindex i identifies the signature value in the protocol description.

- $c_{entity,j} = P_{entity}(m)$: Encryption c of message m under the public key of $entity$. Subindex j identifies the encrypted value in the protocol description.

3.2 System set-up

The proposed scheme requires that *students*, *teachers* and the *manager* have a key pair of a public key cryptosystem.

- (P_T, S_T) *teacher*'s key pair.

- (P_S, S_S) *student*'s key pair.

- (P_M, S_M) *manager*'s key pair.

Each key pair must be certified, we assume the use of a Public Key Infrastructure (PKI), as it is proposed in [9].

3.3 Setting up an exam

The *teacher* and the *manager* do the following steps to set up an exam.

Protocol 1

1. *The* teacher *performs the following actions:*
   (a) *Compute a unique examination identifier,* Id, *composed by the following data:*
   - $\mathcal{S}$: *subject name.*
   - $\mathcal{S}c$: *Subject code.*
   - $\mathcal{Q}$: *Semester*
   - $\mathcal{D}$: *Exam date.*
   - $\mathcal{T}$: *Fixed time to answer the exam.*
   - $\mathcal{N}$: *Exam serial number.*

   (b) *Propose the exam questions,* $\mathcal{E}$.

   (c) *Compute the digital signature of* Id *and* $\mathcal{E}$ *with* S_T, $s_{T,1} = S_T(Id, \mathcal{E})$.

   (d) *Encrypt* Id, $\mathcal{E}$ *and* $s_{T,1}$ *using the managers' public key* P_M, $c_{M,1} = P_M(Id, \mathcal{E}, s_{T,1})$.

   (e) *Authenticate himself to the* manager *using his key pair* (P_T, S_T).

   (f) *Send* $c_{M,1}$ *to the* manager

2. *The* manager *performs the following actions:*
   (a) *Decrypt* $c_{M,1}$ *using* S_M *and obtain* Id, $\mathcal{E}$ *and* $s_{T,1}$.

   (b) *Verify the digital signature* $s_{T,1}$ *using the* teacher*'s public key* P_T.

   (c) *Store* $c_{M,1}$ *in a secure way, bound to the exam* Id.

3.4 Beginning, holding and submitting the exam

The *student*, *teacher* and *manger* use the Protocol 2 in order to perform an exam.

Protocol 2

1. *The* teacher *publishes the exam identifier,* Id.

2. *The* student *authenticates herself using her key pair* (P_S, S_S).

3. *The* student *asks for the exam* Id *to the* manager.

4. *The* manager *performs the following steps:*

(a) *Verify if the* student *is registered in the subject $\mathcal{S}$. Each subject in one semester has n students registered. This information is stored by the* manager.

(b) *Check if the current date $\mathcal{D}'$ and time $\mathcal{T}'$ are in the fixed time to answer the exam $\mathcal{D}$ and $\mathcal{T}$ ($\mathcal{D}$ and $\mathcal{T}$ are in the Id).*

(c) *If the previous verifications succeed:*

i. *Decrypt $c_{M,1}$ using S_M and obtain Id, $\mathcal{E}$ and $s_{T,1}$.*

ii. *Encrypt Id, $\mathcal{E}$ and $s_{T,1}$ using P_S, $c_{S,2} = P_S(Id, \mathcal{E}, s_{T,1})$.*

iii. *Send $c_{S,2}$ to the* student.

(d) *Otherwise, return an error code to the* student.

5. *The* student *obtains and verifies the exam questions, solves it and submits the exam answer in the following way:*

(a) *Decrypt $c_{S,2}$ using S_S and obtain Id, the exam questions $\mathcal{E}$, and $s_{T,1}$.*

(b) *Verify the digital signature $s_{T,1}$ using P_M.*

(c) *Write down the exam answer, $\mathcal{A}$.*

(d) *Obtain at random an answer identifier, Ia.*

(e) *Compute the digital signature of $s_{T,1}$, Ia and $\mathcal{A}$ using S_S, $s_{S,2} = S_S(s_{T,1}, Ia, \mathcal{A})$.*

(f) *Encrypt Id, $\mathcal{E}$, $s_{T,1}$, Ia, $\mathcal{A}$ and $s_{S,2}$ using P_M, $c_{M,3} = P_M(\mathcal{E}, Id, s_{T,1}, Ia, \mathcal{A}, s_{S,2})$.*

(g) *Send $c_{M,3}$ to the* manager.

6. *The* manager *performs the following steps:*

(a) *Decrypt $c_{M,3}$ using S_M and obtain $\mathcal{E}$, Id, $s_{T,1}$, Ia, $\mathcal{A}$, and $s_{S,2}$.*

(b) *Check if the current date $\mathcal{D}''$ and time $\mathcal{T}''$ are in the fixed time to answer the exam $\mathcal{D}$ and $\mathcal{T}$.*

(c) *Verify if the* student *has submitted an exam answer previously.*

(d) *If the previous verifications succeed:*

i. *Verify the digital signatures $s_{T,1}$ and $s_{S,2}$ using P_T and P_S respectively.*

ii. *Obtain the current time t.*

iii. *Compute the digital signature of Id, Ia and t using S_M, $s_{M,3} = S_M(Id, Ia, t)$. $s_{M,3}$ is the exam answer receipt, the proof that* student *has delivered her answer.*

iv. *Send Id, Ia, t and $s_{M,3}$ to the* student.

v. *Obtain at random a masked-answer identifier, Ia'.*

vi. *Compute the digital signature of $s_{T,1}$, Ia' and $\mathcal{A}$ using S_M, $s_{M,4} = S_M(s_{T,1}, Ia', \mathcal{A})$.*

vii. *Encrypt $\mathcal{E}$, Id, $s_{T,1}$, $\mathcal{A}$, Ia' and $s_{M,4}$ using P_T, $c_{T,4} = P_T(\mathcal{E}, Id, s_{T,1}, \mathcal{A}, Ia', s_{M,4})$.*

viii. *Store securely, $c_{M,3}$, $s_{M,3}$, Ia, Ia', t and $c_{T,4}$ as one answer of the exam Id. Each exam answer is linked to the* student *who has sent it.*

(e) *Otherwise, return an error code to the* student

7. *The* student *does the following steps:*

(a) *Verify the digital signature $s_{M,3}$ using P_M.*

(b) *Store Id, Ia, t and $s_{M,3}$ as the examination receipt.*

3.5 Grading of exams

The *teacher* and the *manager* use Protocol 3 in order to grade one exam answer.

Protocol 3

1. *The* teacher *performs the following steps:*

(a) *Authenticate himself to the* manager *using his key pair (P_T, S_T).*

(b) *Request for one answer of a given exam Id.*

2. *The* manager *does the following steps:*

(a) *Obtain one exam answer that has not been graded previously, $c_{T,4}$.*

(b) *Send $c_{T,4}$ to the* teacher.

3. *The* teacher *does the following steps:*

(a) *Decrypt $c_{T,4}$ using S_T and obtain $\mathcal{E}$, Id, $s_{T,1}$, $\mathcal{A}$, Ia' and $s_{M,4}$.*

(b) *Verify the digital signature $s_{M,4}$ with P_M.*

(c) *Grade the answer $\mathcal{A}$ with a value $\mathcal{G}$.*

(d) *Compute the digital signature of $\mathcal{E}$, Id, $s_{T,1}$, $\mathcal{A}$, Ia' and $\mathcal{G}$ using S_T, $s_{T,5} = S_T(\mathcal{E}, Id, s_{T,1}, \mathcal{A}, Ia', \mathcal{G})$.*

(e) *Encrypt Id, $\mathcal{E}$, $s_{T,1}$, $\mathcal{A}$, Ia', $s_{M,4}$, $\mathcal{G}$ and $s_{T,5}$ using P_M, $c_{M,5} = P_M(\mathcal{E}, Id, s_{T,1}, \mathcal{A}, Ia', s_{M,4}, \mathcal{G}, s_{T,5})$.*

(f) *Send $c_{M,5}$ to the* manager.

4. *The* manager *does the following steps:*

(a) *Decrypt $c_{M,5}$ using S_M obtaining $\mathcal{E}$, Id, $s_{T,1}$, $\mathcal{A}$, Ia', $s_{M,4}$, $\mathcal{G}$ and $s_{T,5}$.*

(b) *Verify the digital signatures $s_{T,1}$, $s_{M,4}$ and $s_{T,5}$ with P_T, P_M and P_T respectively.*

(c) *Obtain the $c_{M,3}$ that corresponds to $c_{T,4}$. The manager has stored $c_{M,3}$ and Ia', so using Ia' can find the $c_{M,3}$ linked to $c_{T,4}$, i.e. the student's answer.*

(d) *Decrypt $c_{M,3}$ using S_M, and obtain $\mathcal{E}$, Id, $s_{T,1}$, Ia, $\mathcal{A}$ and $s_{S,2}$.*

(e) *Encrypt $\mathcal{E}$, Id, $s_{T,1}$, Ia, $\mathcal{A}$, $\mathcal{G}$, $s_{S,2}$ and $s_{T,5}$ using P_S, $c_{S,6} = P_S(\mathcal{E}, Id, s_{T,1}, Ia, \mathcal{A}, \mathcal{G}, s_{S,2}, s_{T,5})$.*

(f) *Store $c_{S,6}$, Id and Ia in a secure way.*

3.6 Obtaining the score of the exam answer

The *student* obtains her exam score by running the Protocol 4 together with the *manager*.

Protocol 4

1. *The* student *authenticates herself in front of the* manager *using her key pair (P_S, S_S).*

2. *The* student *requests from the* manager *the score of the answer Ia.*

3. *The* manager *performs the following steps:*

   (a) *Verify if Ia belongs to the* student *that has been authenticated.*

   (b) *Obtain $c_{S,6}$ that had been stored;*

   (c) *Send $c_{S,6}$ to the* student.

4. *The* student *obtains the grade $\mathcal{G}$ by following the next steps:*

   (a) *Decrypt $c_{S,6}$ using S_S, and obtain $\mathcal{E}$, Id, $s_{T,1}$, Ia, $\mathcal{A}$, $\mathcal{G}$, $s_{S,2}$ and $s_{T,5}$.*

   (b) *Verify the digital signatures $s_{T,1}$, $s_{S,2}$ and $s_{T,5}$ using P_T, P_S and P_T respectively.*

3.7 Revising of exams

The *student* may apply for an exam grade revision by running the Protocol 5 together with the *manager*.

Protocol 5

1. *The* student *does the following steps:*

   (a) *Authenticate herself in front of the manager using her key pair (P_S, S_S).*

   (b) *Obtain at random one number that will be the revision identifier, Ir.*

   (c) *Compute a digital signature of Id, Ia, Ir using S_S, $s_{S,6} = S_S(Id, Ia, Ir)$. $s_{S,6}$ is the request to review the score of the answer Ia.*

   (d) *Send Id, Ia, Ir and $s_{S,6}$ to the* manager.

2. *The* manager *does the following steps:*

   (a) *Verify the digital signature $s_{S,6}$ using P_S.*

   (b) *Store Id, Ia, Ir and $s_{S,6}$.*

The *teacher* uses a modification of Protocol 3 in order to review one exam.

4 Security analysis

We assume that the *manager* is honest, so our protocol is based on a Trusted Third Party (TTP), that is the *manager*. The *manager* is protected with conventional security measures (firewalls, VPN, IDS, etc...) described in [6, 5, 3, 14].

Authenticity:

- In Step 1c of Protocol 1 the teacher digitally signs the exam. The student verifies this signature in Step 5b of Protocol 2, and then she gets sure that the exam questions have been proposed by the teacher.
- In Step 3d of Protocol 3 the teacher digitally signs the grade. The student verifies the digital signature in Step 4b of Protocol 4, so she is convinced that grade has been proposed by the teacher.
- In Step 5e of Protocol 2 the student digitally signs the exam answer. The manager verifies the student's signature in Step 6(d)i of Protocol 2 and computes a digital signature of exam answer in Step 6(d)vi. The teacher verifies the manager's digital signature in Step 3b of Protocol 3. Assuming *manager* honesty, the teacher has no doubt the answer has been written by a valid student.

Privacy:

- In Step 3a of Protocol 3 the teacher receives an exam answer $c_{T,4}$, and he decrypts it obtaining $\mathcal{E}$, Id, $s_{T,1}$, $\mathcal{A}$ and $s_{M,4}$. This information does not reveal the student identity. However, the digital signature $s_{M,4}$ convinces the teacher that $\mathcal{A}$ belongs to a valid student.

Correction:

- In Step 1c of Protocol 1 the teacher digitally signs the exam obtaining $s_{T,1}$. The student computes the digital signature of $s_{T,1}$, Ia and $\mathcal{A}$ in Step 5e of Protocol 2 obtaining $s_{S,2}$. The digital signatures $s_{T,1}$ and $s_{S,2}$ grant that the exam questions have not been modified once the exam has started.

- In Step 6b of Protocol 2 the manager verifies whether the examination time has finished, rejecting any exam answer submission once the time has expired.
- The student digitally signs the exam answer in Step 5e of Protocol 2. So, if the answer is modified the digital signature verification will fail.
- In Step 6c of Protocol 2 the manager verifies if the student has previously delivered an exam answer, and in this case, the exam answer is not accepted.
- If one exam is deleted there is one student that will not obtain her grade, so the deletion is detected. Moreover, the student can prove that she has delivered the exam, because she can show the examination receipt obtained in Step 7 of Protocol 2.

Secrecy:

- The teacher encrypts the exam questions in Step 1d using the *manager*'s public key. The *manager*'s private key is needed to obtain the exam questions, and such key is restricted to the *manager*. The *manager* sends the exam questions to the *student* in Step 4(c)iii of Protocol 2, if the student is registered in the exam subject and if the current time and date are in the fixed time to answer the exam, Steps 4a and 4b of the Protocol 2.
- The *teacher* can deliver the exam solution to the *manager* using a modification of Protocol 1, so the solution is encrypted and only can be obtained by the *manager*.
- In Step 5f of Protocol 2 the *student* encrypts her answer using the *manager*'s public key. At this point, the exam answer only can be obtained by the *manager*. Later on, the *manager* encrypts the exam answer with the *teacher*'s public key in Step 6(d)vii. The teacher obtains the encrypted exam answer in Step 3. We conclude that students' answers are kept secret, so only the teacher and the manager have access to them.
- The *manager* authenticates the Student in Step 1 of Protocol 4 and verifies that she is the owner of the answer Ia in Step 3a of Protocol 4. If the above verification suceed the *manager* sends c_6 to the *student*. c_6 is the exam grade encrypted using the *student*'s public key, so that only the *student* can obtain her grade.

Receipt: The student obtains a receipt in Step 7 of Protocol 2 as a proof of exam delivery.

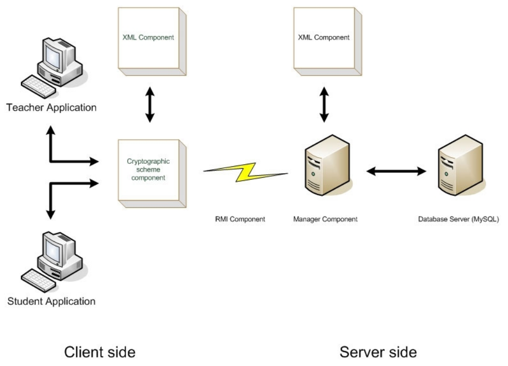

Figure 1. System overview

Copy detection is prevented: The exam takes place in a supervised environment, so the copy detection is prevented using traditional means.

5 Implementation

The secure e-exam management system described in these previous sections has been implemented in a Master Thesis [2]. The system has been developed using Java language because it is platform independent and thus can be deployed in any architecture. Also, Java language offers several cryptographic APIs with the crypto-systems needed in our system. We have used the IAIK [8] library because it contains an implementation of the whole Java Cryptography Extension (JCE) Framework, together with a great documentation. The system is composed of five main components: cryptographic scheme component, XML, RMI, DataBase and finally the graphic interface. In figure 1 we can see the system overview.

5.1 Cryptographic scheme component

The cryptographic scheme contains the implementation of the cryptographic operations presented in Section 3. Each of the clients, *student* and *teacher*, has its own application. Each application has different classes that contain the implementation of the necessary protocols to perform the cryptographic operations.

5.2 XML component

The outputs of the cryptographic scheme component are stored in an XML document using the XML component. XML documents are exchanged between the actors, i.e. *manager*, *student* and *teacher*. Once a document is received, the cryptographic information is obtained using the XML component, and verified using the cryptographic scheme component. If verifications hold the document is stored.

The XML data format allows efficient data management, and, additionally, the system becomes more flexible in terms of updating or modification.

Our implementation uses the JDOM [7] API in the XML component, because it is open source and provides a low-cost entry point for using XML.

5.3 RMI component

To be able to create a distributed system, the Java Remote Method Invocation (Java RMI) [13] technology has been used. In this way, methods of remote Java Objects can be invoked from other Java virtual machines on different hosts. In this way, communication between the *manager*, *student* and *teacher* is transparent and implementation becomes easier.

5.4 DataBase component

The exam questions, answers, grades, and reviews must be stored in a persistent way. Moreover, we need to keep information about *teachers* and *students*.

The system stores the above information in a MySQL [10] DataBase server. Such database has been chosen since it is open source, and there are implementations available for the main architectures, Microsoft© Win32, Linux, and MacOSX ©.

The DataBase (DB) is not accessed directly. The DataBase component is the middleware between the DB and the other system components.

5.5 Graphic interface component

In this master thesis prototype a basic graphical interface has been developed. This interface permits users to perform the basic operations described in Section 2 in an intuitive way.

We have used the Standard Widget Toolkit (SWT), because it is easy to use and is open source.

As pointed out previously, each user has a key pair. The system stores such keys in a PKCS#12 [11] file. In the first step, in any of the two applications (student or teacher), the user must introduce her PKCS#12 file and the password used to protect it. Figure 2 shows the dialog in which the user enters the above information.

Figure 3 displays the *teacher*'s application. In the upper left side there is the exam identifier information. In the upper right side there are the control buttons: create exam, obtain answers, grade answer, and obtain revisions. The << and >> buttons allow to obtain the next exam answer or the next exam that must be reviewed. In the middle of the application there are the exam questions, and below there is the exam answer.

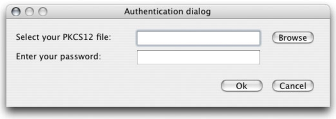

Figure 2. Users' authentication dialog

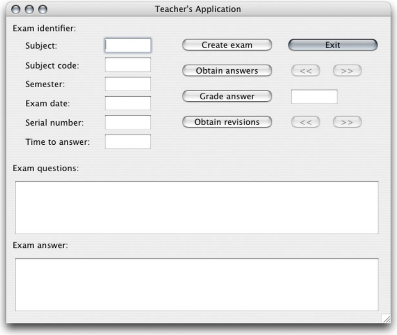

Figure 3. Teacher's application

Figure 4 shows the *student*'s application. In the upper left side, like in the *teacher*'s application, there is the exam identifier information. The control buttons are in the upper right side. The control buttons are the following: get exam, get exam grade, send answer and ask for revision. The exam questions and the space to introduce the exam answer are in the same layout as in the *teacher*'s application.

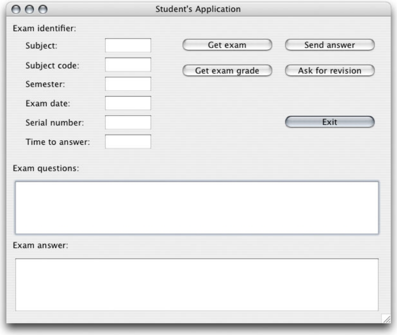

Figure 4. Student's application

6. Conclusions

In this paper we have presented a secure e-exam management system. We have reviewed all exam stages and we have identified the different security properties that every exam stage must satisfy. Such information has allowed us to define a system based on different cryptographic protocols that offer a high security level for all exam stages. Moreover, the scheme has been implemented in [2], in order to test its functionality and some implementation details have been presented. However, the proposed system assumes that in the setting up stage, students hold the exam in a supervised environment. Further research should be directed to allow students to hold exams in a less restricted environment.

Acknowledgements and disclaimer

This work is partially supported by the Spanish MCYT and the FEDER funds under grant SEG2004-04352-C04-04 PROPRIETAS-WIRELESS. The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. The first author is partly supported by the Catalan Government under grant 2005 SGR 00446, and by the Spanish Ministry of Science and Education through project SEG2004-04352-C04-01 "PROPRIETAS".

References

[1] D. Chadwick, R. Tassabehji, and A. Young. Experiences of using a public key infrastructure for the preparation of examination papers. *Computers & Education*, 35(1):1–20, august 2000. ISSN: 0360-1315.

[2] A. Dorca-Josa. Cryptographic scheme for secure e-exams. Master's thesis, Universitat Oberta de Catalunya, january 2005. Language: catalan.

[3] K. El-Khatib, L. Korba, Y. Xu, and G. Yee. Privacy and security in e-learning. *International Journal of Distance Education*, 1(4), October-December 2003. ISSN: 1539-3100.

[4] Exon Gurukul Online, Learning Solutions, Online Examinations©. http://www.gurukulonline.com, 2005.

[5] S. Furnell, U. Bleimann, J. Girsang, H. Rder, P. Sanders, and I. Stengel. Security considerations in online distance learning. In W. Hahn, E. Walther-Klaus, and J. Knop, editors, *Proceedings of Euromedia 99*, pages 31–135,, Munich, Germany, 25-28 April 1999. ISBN 1-56555-169-9.

[6] S. Furnell, P. Onions, U. Bleimann, U. Gojny, M. Knahl, H. Rder, and S. P. A security framework for online distance learning and training. *Internet Research*, 8(3):236–242, 1998. ISSN: 1066-2243.

[7] J. Hunter and B. McLaughlin. The jdom xml api. http://www.jdom.org/docs/apidocs/index.html.

[8] (IAIK-JCE). The iaik java cryptography extension. http://jce.iaik.tugraz.at/sic/products/core_crypto_toolkits/jca_jce.

[9] G. Kambourakis, K. D-P.N., A. Rouskas, and S. Gritzalis. A pki approach for deploying modern secure distributed e-learning and m-learning environments. *Computers & Education*, Article in press. ISSN: 0360-1315.

[10] MySQL. The mysql database server documentation. http://www.mysql.com/documentation/index.html.

[11] PKCS#12. Personal information exchange syntax standard. http://www.rsasecurity.com/rsalabs/node.asp?id=2138.

[12] Software Secure, Securexam©. http://www.softwaresecure.com/, 2005.

[13] Sun-Microsystems. The java remote method invocation documentation. http://java.sun.com/products/jdk/rmi/reference/docs/index.html.

[14] E. Weippl. *Security in E-Learning*, volume 16 of *Advances in Information Security*. Springer Science+Business Media, Inc., 2005. ISBN: 0-387-24341-0.