Implementing Data Security in Student Lifecycle Management System at the University of Prishtina

BLERIM REXHA
HAXHI LAJQI
MYZAFERE LIMANI
Faculty of Electrical and Computer Engineering
University of Prishtina
Kodra e Diellit pn., 10000 Prishtina
KOSOVO
blerim.rexha@fiek.uni-pr.edu, haxhi.lajqi@fiek.uni-pr.edu, myzafere.limani@fiek.uni-pr.edu
www.uni-pr.edu/fiek

Abstract: - In this paper is presented a novel approach for fulfilling the data security criteria in a Student Lifecycle Management System at the University of Prishtina. The four main criteria of data security such as: privacy, authentication, integrity and non-repudiation are fulfilled through carefully selected security policies. Student data privacy is achieved using the Secure Socket Layer protocol for web communication with web server. Each user, being student, academic or administrative staff is provided with unique user name and initial password in the Student Lifecycle Management System. Data integrity and non-repudiation are fulfilled using digital signatures. The novelty of implemented solution is based on extending the subject name in X.509 digital certificates and using this certificate for securing student grades, which is in full compliance with the Kosovo Law on Information Society. Public Key Infrastructure and X.509 digital certificates have been established as the most trustworthy methods for assuring data security criteria in modern software applications. Security policy enforces that digital certificate and its associated private key shall be stored in a smart card. Access to private key stored in a smart card is protected by Personal Identification Number, known only by smart card holder. This implementation was installed at the Faculty of Electrical and Computer Engineering and has successfully passed a six semester testing period and students were, for the first time in the history of the University of Prishtina, able to apply online to take an exam.

Key-Words: - Authentication**,** Digital Signature, Non-Repudiation, Privacy, Security, Smart Cards, Student Lifecycle Management, X.509 Certificate

1 Introduction

The University of Prishtina is established in accordance with the Law on the Establishment of the University (Official Journal of SAP Kosovo no. 33/69) on 18 November 1969 and is the only public university in Kosovo. It is governed based on the Law on Higher Education, L2003-14 adopted by Assembly of Kosovo in 2003 and “Statute of the University” approved by university senate in July 2004 [1]. The University of Prishtina consists of 17 faculty units located in different cities around Kosovo and has around 30.000 students. In the Table 1 are presented the detailed data about the University of Prishtina of the academic year 2007/08, where the number of enrolled students is increasing yearly [2].

Table 1: Number of students, academic and administrative staff in University of Prishtina

Students	Academic staff	Administrative staff	Academic Units	Courses	Exams Term/Year	Graduated students/Year
28.318	1.055	61	17	2500	5	1500

One of the main challenges of the university's management is the increasing demand for more efficient student services, using modern technologies such as Internet to avoid poor services (in manual and paper form) provided to students during enrollment periods, as well as the abuse of student exam grades by local administrative staff. All student grades by law are to be kept in written form in different records. The procedures are very complicated and sometimes are overlapped and introduce another weak point in the Student Lifecycle Management System (SLMS). Paper records can be lost, duplicated and even can even be forged by a misuser. During the main exam periods, as defined by the statute of the university, there is an increase in demand for student services, and students must apply for an exam in the paper form. One can just imagine the student crowds and the hourly-long queues in front of the faculty administrative desks, as presented in Fig. 1, taken in January 2007 at the Faculty of Electrical and Computer Engineering (FECE) administration office.

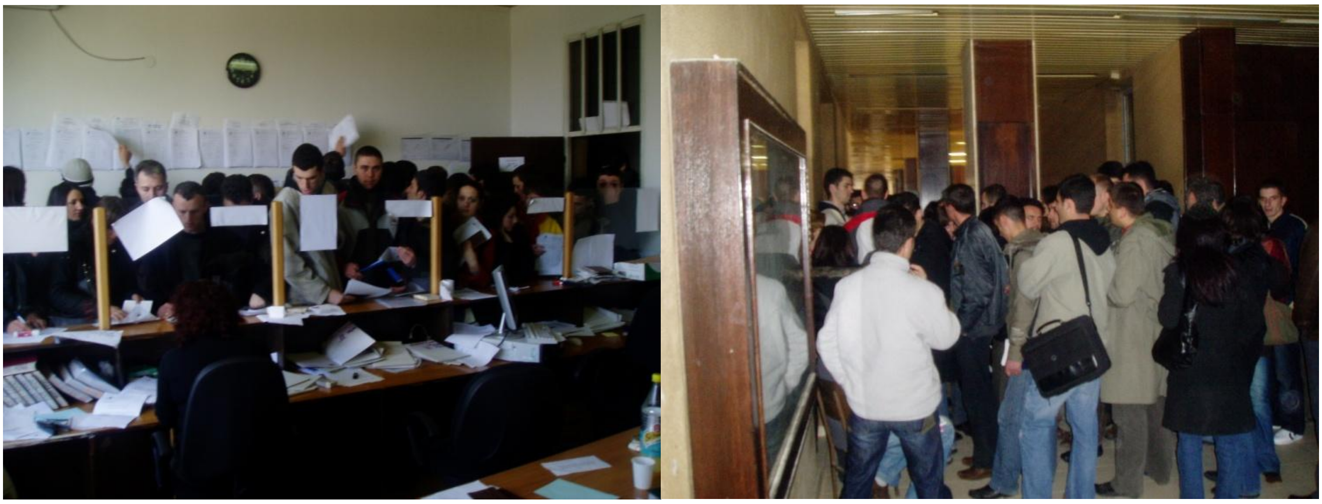


Fig. 1: Student crowd stretching from administrative office to the faculty doorway

Modernizing the student services in general become the highest priority for the management of the university, in general to the management of the university were proposed two approaches:

1. Changing the statute of the university, i.e. changing the "business logic" of the university that meets one of the standard "out of the shelf software products" in market, or
2. Implement the customized SLMS that reflects the statute of the University of Prishtina.

Clearly, the management of the university decided for the customized SLMS and a pilot project was started in November 2007 at the FECE.

2 The Paper Form Procedures

Since from its begging the University of Prishtina has introduced a very comprehensive paper form procedure for ensuring the quality of its business processes. This paper form procedures might be very modern in late '70 in late century but now nowadays these paper form procedures are obstacle to shift business process toward more efficient and competitive student services.

2.1 Applying to take an exam in the paper form

During the pre-exam period, students must apply in paper form to register to take the exam. This pre-exam period is usually 2 till 5 days. This paper form consists of several fields that have to be filled by the student, such us: student name, student ID, course number and title, lecturer name and actual date. The administrative staff of the faculty collects these application forms and divides them based on lecturer and course title. At the exam time, the back of this registration form must be filled by the lecturer, with information regarding the student grade, grades for the oral and written part, the exam date, and finally, must be signed by the lecturer.

2.2 Saving the student grades in paper form

Once the exam paper forms are completed by the lecturer, they are handed over to administrative staff, which in turn has to copy by hand the grade into the faculty main book and save this from the paper form to a paper student file [1]. Later on when the student needs a grade transcript of his record, the faculty clerk has to open the main faculty book and from there prescribe the student grades. This is very hard work and is prone to much misuse, as well as sometimes may require hours of searching through all records in the faculty main book.

Having in mind that large number of students that university has, each faculty has at least 4-6 administrative clerks that have access to the faculty main book. Even the handwritten signature can be link to them individually this is still very easy to forge. The security of this system is left as the personal responsibility of the administrative clerk, since to forge a handwritten signature is an easy job. Thus the student file saved only in the paper form presents a weak point of SLMS.

The management of the university has set itself as a high priority the avoidance of using this practice, and the introduction of a new student services using modern technologies and protocols, such as user authentication and non-repudiation using digital signature for assuring data security and the applying for an exam via the Internet.

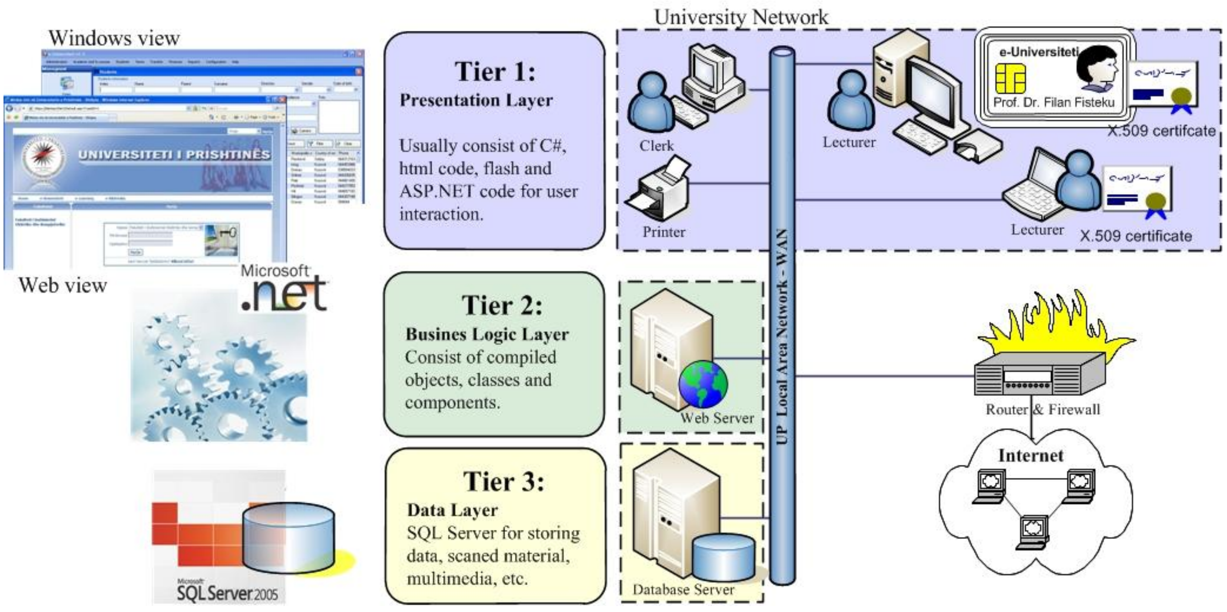
3 Shifting to Digitalization and Internet

The University of Prishtina has its university network in place, as in details described in [3], its all faculty units are connected over the Local Area Network (LAN) with central administration.

3.1 Application architecture

In the Fig. 2 is presented the general architecture of the SLMS software solution. This solution was implemented by a local software company in Prishtina, Kosovo. The SLMS was developed with three tier architecture, standard model architecture as described in [4], whereby the Microsoft SQL Server was used as database management system and Microsoft's Internet Information Service (IIS) as application server. Similar three tier approach is also used by [5]. The FECE management is considering to supply the data room, where are installed the server, with green energy, since Kosovo has a modest potential on renewable energy, as described in [6]. The SLMS, as is depicted in Fig. 2, has two views:

1. Windows form (application) – which is used by the faculty staff to manage the teaching courses and inserting student grades into the system, and
2. Web view – used by students to check their records and apply for an exam via the Internet. The web communication is secured by the Secure Socket Layer (SSL) protocol.



Usually consist of C#, html code, flash and ASP.NET code for user interaction.

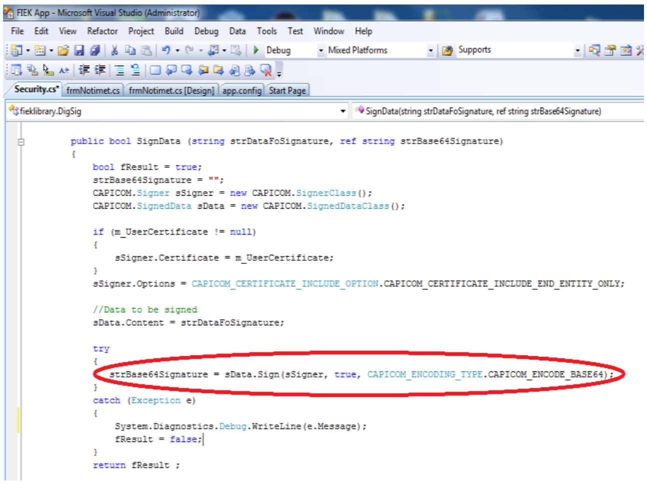
Consist of compiled objects, classes and components.

SQL Server for storing data, scaned material, multimedia, etc.

Fig. 2: General network infrastructure of SLMS

3.2 Windows application

The Windows application was developed using C# programming language and the latest Microsoft .NET runtime environment. Microsoft Cryptographic Application Interface Component Object Module (CAPICOM) has been used for the creation of the digital signature, as presented in Fig. 3.


FIEK App - Microsoft Visual Studio (Administrator)
File Edit View Refactor Project Build Debug Data Tools Test Window Help
Debug
Mixed Platforms
Supports
Security.cs*
frmNotimet.cs
frmNotimet.cs [Design]
app.config
Start Page
fieklibrary.DigSig
SignData(string strDataFoSignature, ref string strBase64Signature)

```
        public bool SignData (string strDataFoSignature, ref string strBase64Signature)
        {
            bool fResult = true;
            strBase64Signature = "";
            CAPICOM.Signer sSigner = new CAPICOM.SignerClass();
            CAPICOM.SignedData sData = new CAPICOM.SignedDataClass();

            if (m_UserCertificate != null)
            {
                sSigner.Certificate = m_UserCertificate;
            }
            sSigner.Options = CAPICOM_CERTIFICATE_INCLUDE_OPTION.CAPICOM_CERTIFICATE_INCLUDE_END_ENTITY_ONLY;

            //Data to be signed
            sData.Content = strDataFoSignature;

            try
            {
                strBase64Signature = sData.Sign(sSigner, true, CAPICOM_ENCODING_TYPE.CAPICOM_ENCODE_BASE64);
            }
            catch (Exception e)
            {
                System.Diagnostics.Debug.WriteLine(e.Message);
                fResult = false;
            }
            return fResult ;
```

Fig. 3: Using CAPICOM in source code of SLMS

The application was installed in each client computer, i.e. faculty staff: academic and administrative staff. Each academic staff entitled to grade students has received a digital X.509 certificate issued by a local Certification Authority (CA) trust center in Prishtina, Kosovo. Also in client computer the root certificates from CA are installed in “Trusted Root Certification Authorities” store. To each professor’s computer is installed an Omnikey 3121 USB desktop smart card reader. The communication with smart card reader is based on standard Personal Computer Smart Card (PC/SC) interface. The SLMS is not only a central point for student administration but also for generating very sophisticated student reports required the management of the university such as student course participation, student success and grade distribution as presented in [4]. Furthermore the SLMS enabled the management of the faculty, i.e. the dean that in one “click” to have all necessary information about quality of grading process as well as for other financial and administrative information.

3.3 Web application

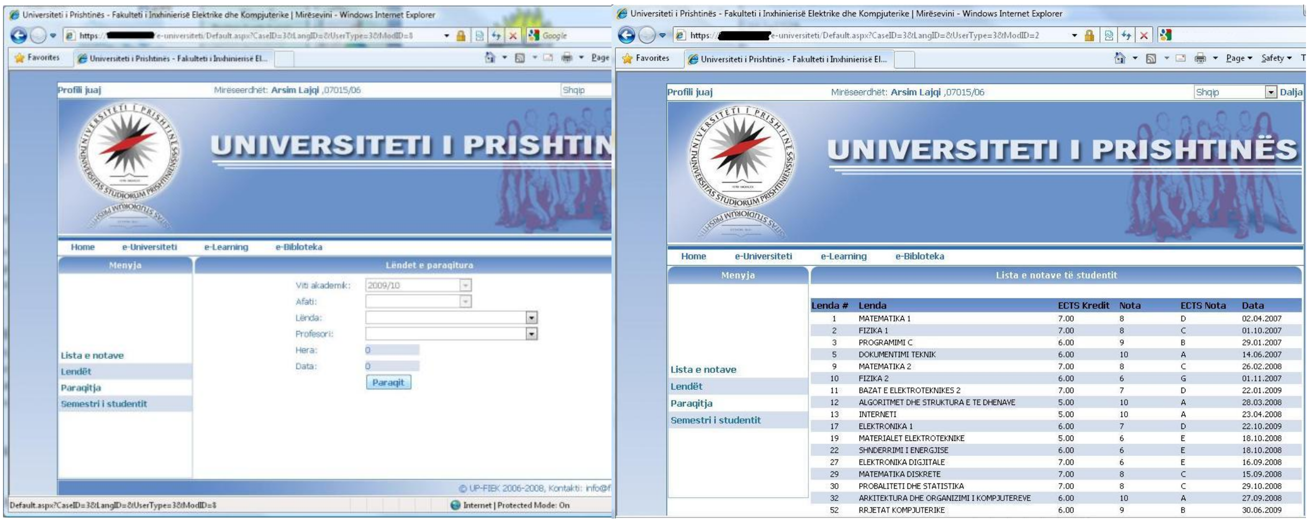
The web application was developed using Microsoft Developer Studio 2005 and recently ported to 2008 version and C# and Active Server Pages (ASP) as programming language. Furthermore AJAX (Asynchronous JavaScript and XML) is used as ASP.NET extension to make the SLMS user interface more interactive and dynamic. This application is used only by students. During the enrollment process to each student is assigned a unique username and an initial password that that must be changed at the first login. Changing of the initial password is enforced by security policy. Through this application, a student will be able to apply for an exam, receive the exam results and see his student file, i.e. grade transcript over the Internet, as is presented in Fig. 4. Grade transcript used to be a nightmare requirement by students for administrative staff before SLMS. Usually there were grades missing in the faculty main book, because the academic staff i.e. the professor has forgotten them to bring to administrative office or simply professor did not filled the exam application paper form yet. Thus students had many complains about the administrative staff and their grade transcript. With SLMS via Internet they see the exact copy of the grade transcript that the faculty administrative staff will issue to them.

The main feature of the web SLMS is applying to take an exam via Internet. Having in mind the student data presented in Table 1, one can calculate the student transport savings per year as:

$$\frac{1}{2} * NrOfStudents * NrOfExamTerms * 1Euro = \qquad (1)$$

$$\frac{1}{2} * 28.318 * 5 * 1Euro = 70.790Euro$$

Where in formula (1) is assumed that only the half of the total number of students live outside university campus and need public transport with an average student ticket price is about 1 Euro.



Universiteti i Prishtinës - Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike | Mirësevini - Windows Internet Explorer

https://[redacted]e-universiteti/Default.aspx?CaseID=3&LangID=&UserType=3&ModID=8

Profili juaj — Mirëseerdhët: Arsim Lajqi ,07015/06

Lëndet e paraqitura

Viti akademik: 2009/10
Afati:
Lënda:
Profesori:
Hera: 0
Data: 0

© UP-FIEK 2006-2008, Kontakti: info@f

Default.aspx?CaseID=3&LangID=&UserType=3&ModID=8

Universiteti i Prishtinës - Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike | Mirësevini - Windows Internet Explorer

https://[redacted]e-universiteti/Default.aspx?CaseID=3&LangID=&UserType=3&ModID=2

Profili juaj — Mirëseerdhët: Arsim Lajqi ,07015/06

Lista e notave të studentit

Lenda #	Lenda	ECTS Kredit	Nota	ECTS Nota	Data
1	MATEMATIKA 1	7.00	8	D	02.04.2007
2	FIZIKA 1	7.00	8	C	01.10.2007
3	PROGRAMIMI C	6.00	9	B	29.01.2007
5	DOKUMENTIMI TEKNIK	6.00	10	A	14.06.2007
9	MATEMATIKA 2	7.00	8	C	26.02.2008
10	FIZIKA 2	6.00	6	G	01.11.2007
11	BAZAT E ELEKTROTEKNIKES 2	7.00	7	D	22.01.2009
12	ALGORITMET DHE STRUKTURA E TE DHENAVE	5.00	10	A	28.03.2008
13	INTERNETI	5.00	10	A	23.04.2008
17	ELEKTRONIKA 1	6.00	7	D	22.10.2009
19	MATERIALET ELEKTROTEKNIKE	5.00	6	E	18.10.2008
22	SHNDERRIMI I ENERGJISE	6.00	6	E	18.10.2008
27	ELEKTRONIKA DIGJITALE	7.00	6	E	16.09.2008
29	MATEMATIKA DISKRETE	7.00	8	C	15.09.2008
30	PROBALITETI DHE STATISTIKA	7.00	8	C	29.10.2008
32	ARKITEKTURA DHE ORGANIZIMI I KOMPJUTEREVE	6.00	10	A	27.09.2008
52	RRJETAT KOMPJUTERIKE	6.00	9	B	30.06.2009

Fig. 4: Applying for exam and grade transcript over web SLMS

4 Fulfilling the Security Criteria in SLCMS

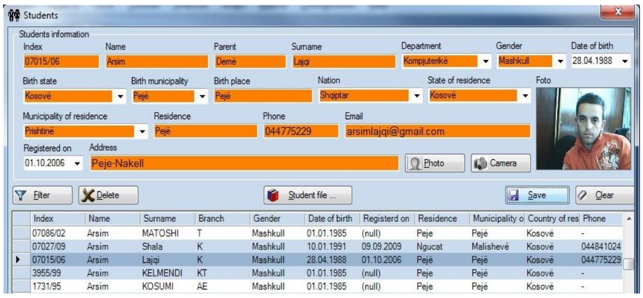
The SLMS was developed having the security features in mind. The SLMS should not only be more efficient in terms of reducing the costs and administrative work but should be more secure as actual paper form management system. Eliminating the grade forging, as the greatest image and quality damager of the public university was a "must have" feature in SLMS. Therefore different cryptographic algorithms were analyzed and implemented in SLMS. Cryptography is the science of writing in secret code. It is, to most people, concerned with keeping communications private. In data storage and telecommunications, cryptography is necessary when communicating over any un-trusted medium, which includes just about any network, particularly the Internet "Cryptography is about communication in the presence of adversaries. As an example a classic goal of cryptography is privacy: two parties wish to communicate privately, so that an adversary knows nothing about what was communicated" [7]. Cryptography provides mechanisms that enable communicating parties to achieve [8]:

- Authentication – the process of proving one's identity,
- Privacy – ensuring that no one can read the message except the intended receiver,
- Integrity – assuring the receiver that the received message has not been changed during transmission, and
- Non-repudiation – preventing the sender from claiming afterwards that he did not send the message.

4.1 User authentication and privacy

The user access to SLMS is controlled through access policy, which has four predefined user groups:

- Student – this group includes all students, and they have the right to access the data only through a web interface,
- Administration – includes faculty administrative staff who can access only administrative data,
- Professor – academic staff of the faculty, who can access only their respective teaching data and each professor possess a X.509 digital certificate, smart card and smart card reader,
- Management – faculty management (dean and vice deans) who have the access rights to create lot of management statistics about the faculty business and quality processes.



Students

Students information

Index	Name	Parent	Surname	Department	Gender	Date of birth
07015/06	Arsim	Demë	Lajqi	Kompjuterikë	Mashkull	28.04.1988

Birth state	Birth municipality	Birth place	Nation	State of residence
Kosovë	Pejë	Pejë	Shqiptar	Kosovë

Municipality of residence	Residence	Phone	Email
Prishtinë	Pejë	044775229	arsimlajqi@gmail.com

Registered on	Address
01.10.2006	Peje-Nakell

Index	Name	Surname	Branch	Gender	Date of birth	Registerd on	Residence	Municipality o	Country of res	Phone
07086/02	Arsim	MATOSHI	T	Mashkull	01.01.1985	(null)	Peje	Pejë	Kosovë	-
07027/09	Arsim	Shala	K	Mashkull	10.01.1991	09.09.2009	Ngucat	Malishevë	Kosovë	044841024
07015/06	Arsim	Lajqi	K	Mashkull	28.04.1988	01.10.2006	Pejë	Pejë	Kosovë	044775229
3955/99	Arsim	KELMENDI	KT	Mashkull	01.01.1985	(null)	Peje	Pejë	Kosovë	-
1731/95	Arsim	KOSUMI	AE	Mashkull	01.01.1985	(null)	Peje	Pejë	Kosovë	-

Fig. 5: Student enrollment form in edit mode

During the student enrollment process using the student enrollment form, as presented in Fig. 5, to each student is assigned a unique username consisting from low case latter "e" (meaning "etudiant" from French language for student) and faculty student unique enrollment ID (so called index number) and a dynamic temporary initial password that that must be changed at the first login. This form can be accessed only by faculty administrative staff. The structure of username and initial password is presented in Fig. 6.

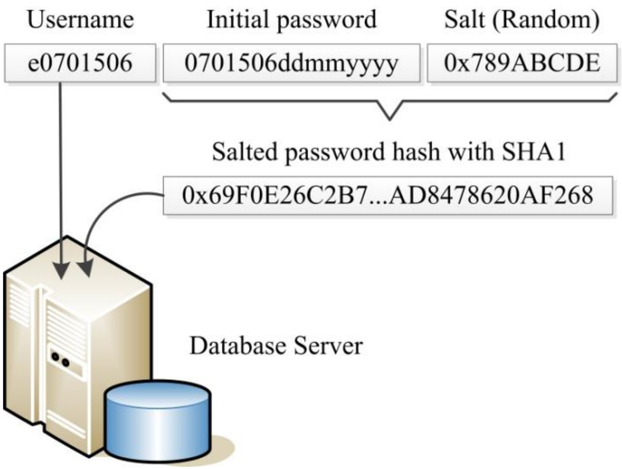


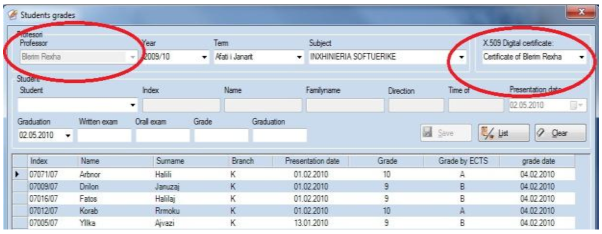
Fig. 6: Username and password structure

The initial password consists of the student ID plus the concatenated string of student birth date, thus is achieved to have personalized initial passwords. *This method has until now, shown no cases of student accounts abuse*. In SLMS database is stored only the salted hash of the student password, as presented in Fig. 6, so no one can retrieve and misuse user passwords. Secure Hash Algorithm v1 (SHA1) is used as hash algorithm. The same security policy applies also for the other user groups. Changing of the initial password is enforced by security policy.

All communication with web server is encrypted by Secure Socket Layer (SSL) protocol, as is presented in Fig. 4, thus protecting the student data from any adversary sniffing the network traffic. Similar approach, authentication with Public Key Infrastructure and X.509 certificates is presented in [9]. The web server certificate is issued also by local trust center in Prishtina, Kosovo and corresponding Trust Center CA is installed in local machine store “Trusted Root Certification Authorities” store.

4.2 Data integrity and non-repudiation

One of the main requirements of the SLMS was the data integrity, i.e. the protection against the misuse of student examination grades. One should have in mind that student grades are stored in database server in clear text. Thus everyone who knows the database password, or is the administrator of the database or domain administrator has the possibility to change these grades in unauthorized form. Therefore, protection to this very popular attack is the approach that each student grade is digitally signed by the professor private key. The Rivest-Shamir-Adelman (RSA) algorithm was chosen as signature algorithm. After professor is logged in SLMS, i.e. authenticating himself with username and password, he has access to his specific courses and can proceed to grade signing form, as presented in Fig. 7. This form will be opened only if professor has in his “User Store” as defined in [10] at least one X.509 digital certificate. As is presented in Fig. 7 the combo box control is read only, i.e. it is automatically filled with data received during the login process identified by logged in user.



Professor: Blerim Rexha
Year: 2009/10
Term: Afati i Janarit
Subject: INXHINIERIA SOFTUERIKE
X.509 Digital certificate: Certificate of Blerim Rexha
Student
Index
Name
Familyname
Direction
Time of
Presentation date: 02.05.2010
Graduation: 02.05.2010
Written exam
Orall exam
Grade
Graduation

Index	Name	Surname	Branch	Presentation date	Grade	Grade by ECTS	grade date
07071/07	Arbnor	Halili	K	01.02.2010	10	A	04.02.2010
07009/07	Drilon	Januzaj	K	01.02.2010	9	B	04.02.2010
07016/07	Fatos	Halilaj	K	01.02.2010	9	B	04.02.2010
07012/07	Korab	Rrmoku	K	01.02.2010	10	A	04.02.2010
07005/07	Yllka	Ajvazi	K	13.01.2010	9	B	04.02.2010

Fig. 7: Signing student grades with X.509 digital certificates

The structure of data to be protected by digital signature is presented in Fig. 8. The “Time” value is actual time taken from executing host and is used to prohibit the possible replay attacks scenarios. If by any case an unauthorized user grants access to the database server, he cannot insert any new record into the data-base because he does not possess the private key needed for the digital signature. This private key is stored only in the smart card of the professor. The private key never leaves the smart card and it can be used for digital signature only after successful Personal Identification Number (PIN) presentation. Three times of unsuccessful presentation of PIN lied the smart card to block the access to private key.

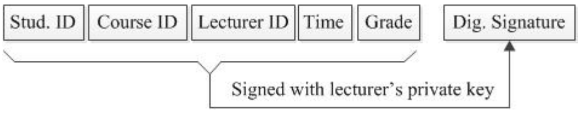
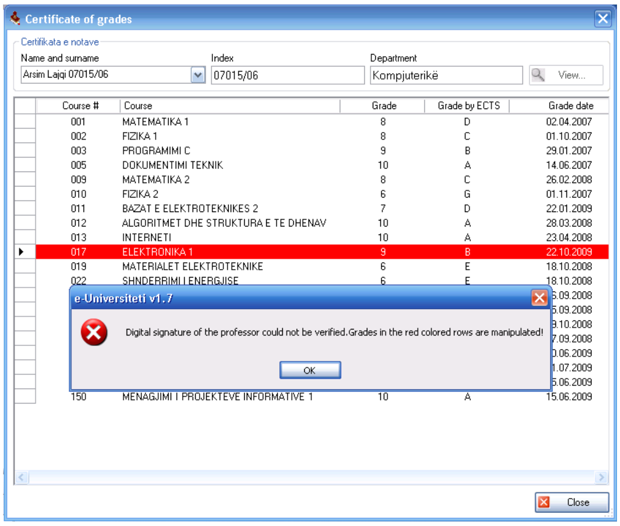


Fig. 8: Structure of signing data

However, what an unauthorized user can do is to forge the student grade. The SLMS is protected against this data inconsistency in the following way: the faculty administrative staff before issuing (printing) any student grade transcript at the administrative office, the digital signature verification module validates the signature over each student grade. If there is misuse, these grades are shown in red color in the application form and the print button is disabled, thus no grade transcript can be issued (printed) to a student, as presented in Fig. 9. In this form the entire responsibility lies with the professor, who is the only person in charge of inserting the examination grades into the database. *Until now, we have not encountered any case of grade misuse*.



Name and surname: Arsim Lajqi 07015/06
Index: 07015/06
Department: Kompjuterikë

Course #	Course	Grade	Grade by ECTS	Grade date
001	MATEMATIKA 1	8	D	02.04.2007
002	FIZIKA 1	8	C	01.10.2007
003	PROGRAMIMI C	9	B	29.01.2007
005	DOKUMENTIMI TEKNIK	10	A	14.06.2007
009	MATEMATIKA 2	8	C	26.02.2008
010	FIZIKA 2	6	G	01.11.2007
011	BAZAT E ELEKTROTEKNIKES 2	7	D	22.01.2009
012	ALGORITMET DHE STRUKTURA E TE DHENAV	10	A	28.03.2008
013	INTERNETI	10	A	23.04.2008
017	ELEKTRONIKA 1	9	B	22.10.2009
019	MATERIALET ELEKTROTEKNIKE	6	E	18.10.2008
022	SHNDERRIMI I ENERGJISE	6	E	18.10.2008
				5.09.2008
				5.09.2008
				9.10.2008
				7.09.2008
				0.06.2009
				1.07.2009
				5.06.2009
150	MENAGJIMI I PROJEKTEVE INFORMATIVE 1	10	A	15.06.2009

e-Universiteti v1.7

Digital signature of the professor could not be verified.Grades in the red colored rows are manipulated!

OK

Fig. 9: Digital signature verification

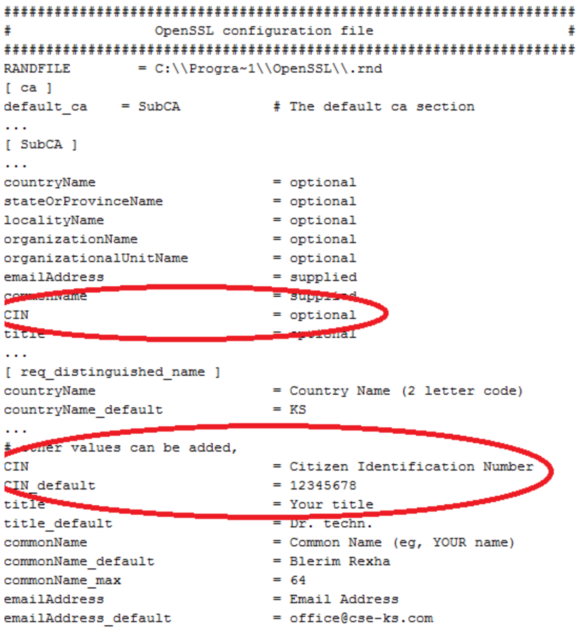
4.3 Key generation and storage

One of the fundamental problems of cryptographic algorithms is the need for tamper resistant and secure storage of keys. Otherwise cracking the encryption algorithms with highly sophisticated and expensive devices would be worthless if the keys are free accessible. The most secure place to store keys is the user's brain [11], but who can or has the will to remember a 1024 or 2048 bit RSA key?

4.3.1 Using OpenSSL

Generation of private and public key is done by OpenSSL software. OpenSSL is a project driven by volunteer programmers to develop an open source toolkit for implementing the SSL, TLS and general purpose cryptographic libraries. OpenSSL is based on the SSLeay library developed by Eric A. Young and Tim J. Hudson. OpenSSL toolkit is free to use for commercial and non-commercial purposes [12]. OpenSSL is a command line driven tool; therefore the challenge was changing the configuration file and writing a script for generating a X.509 certificate and specially inserting proprietary data into subject's name in digital certificate. OpenSSL is standard tool for building governmental Public Key Infrastructure (PKI), as described in [13].

The novelty of the approach implemented in SLMS is that *X.509 digital certificate includes beyond the standard properties also the Citizen Identification Number (CIN) from Kosovo Civil Registry (KCR) within subject's name*. Fig. 10 describes a part of the OpenSSL configuration file, which has the format of a standard INI file, with predefined sections, user defined sections, and values.

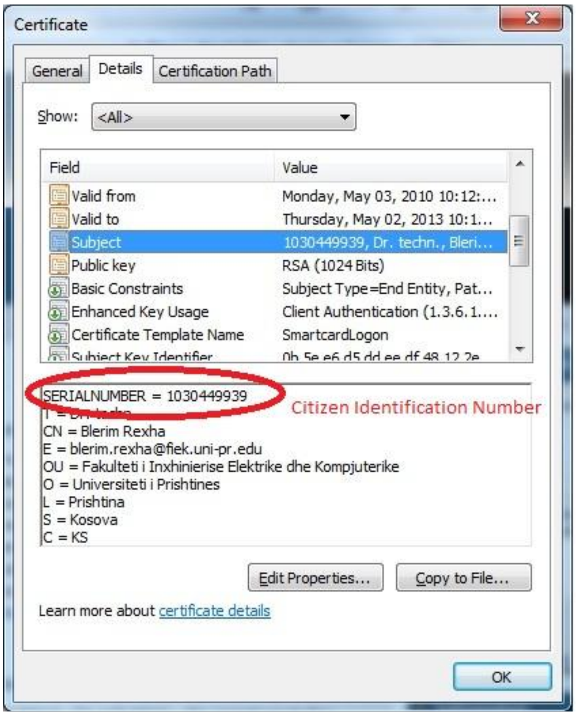


```
####################################################################
#                  OpenSSL configuration file                      #
####################################################################
RANDFILE        = C:\\Progra~1\\OpenSSL\\.rnd
[ ca ]
default_ca    = SubCA            # The default ca section
...
[ SubCA ]
...
countryName                     = optional
stateOrProvinceName             = optional
localityName                    = optional
organizationName                = optional
organizationalUnitName          = optional
emailAddress                    = supplied
commonName                      = supplied
CIN                             = optional
title                           = optional
...
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = KS
...
# other values can be added,
CIN                             = Citizen Identification Number
CIN_default                     = 12345678
title                           = Your title
title_default                   = Dr. techn.
commonName                      = Common Name (eg, YOUR name)
commonName_default              = Blerim Rexha
commonName_max                  = 64
emailAddress                    = Email Address
emailAddress_default            = office@cse-ks.com
```

Fig. 10: OpenSSL configuration file

During the certificate enrollment and face to face authentication process at the registration office at local trust center the CIN number is entered at OpenSSL script. Therefore this X.509 certificate can be used in all upcoming e-Government services, where CIN is required such us bank transactions, tax refunds, civil registry etc. This is in fully in compliance with the latest recommendation of RFC 5280, as described in [14].

Fig. 11 presents e view of such X.509 digital certificate, generated with OpenSSL and customized batch script as presented in Fig. 10.



Show: <All>

Field	Value
Valid from	Monday, May 03, 2010 10:12:...
Valid to	Thursday, May 02, 2013 10:1...
Subject	1030449939, Dr. techn., Bleri...
Public key	RSA (1024 Bits)
Basic Constraints	Subject Type=End Entity, Pat...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Certificate Template Name	SmartcardLogon
Subject Key Identifier	0b 5e e6 d5 dd ee df 48 12 2e

SERIALNUMBER = 1030449939
T = Dr. techn.
CN = Blerim Rexha
E = blerim.rexha@fiek.uni-pr.edu
OU = Fakulteti i Inxhinierise Elektrike dhe Kompjuterike
O = Universiteti i Prishtines
L = Prishtina
S = Kosova
C = KS

Citizen Identification Number

Learn more about certificate details

Fig. 11: Including CIN in a X.509 certificate

4.3.2 Using SICRYPT smart card

A smart card is a portable, tamper-resistant processor with a programmable data store and data processing. It has different size formats, but mostly has the shape and size of a credit card and holds sensitive information in the range from 1 to 64 kilo bytes (KB).

The new smart cards, like the Infineon SLE66CX of SICRYPT family, have a Central Processing Unit (CPU) a 16 bit microcontroller, 64 kB of EEPROM and an Advanced Crypto Engine (ACE) for cryptographic operations such DES, triple DES and RSA operations [15]. The file structure of SICRYPT smart card is presented in the Fig. 12.

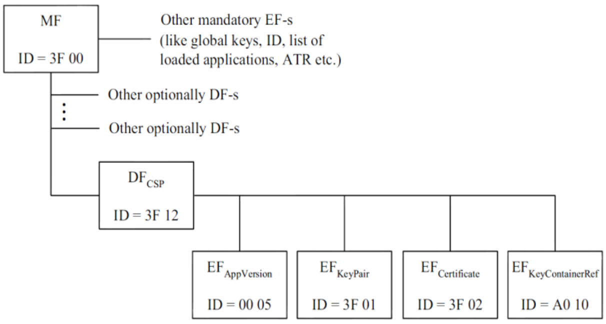
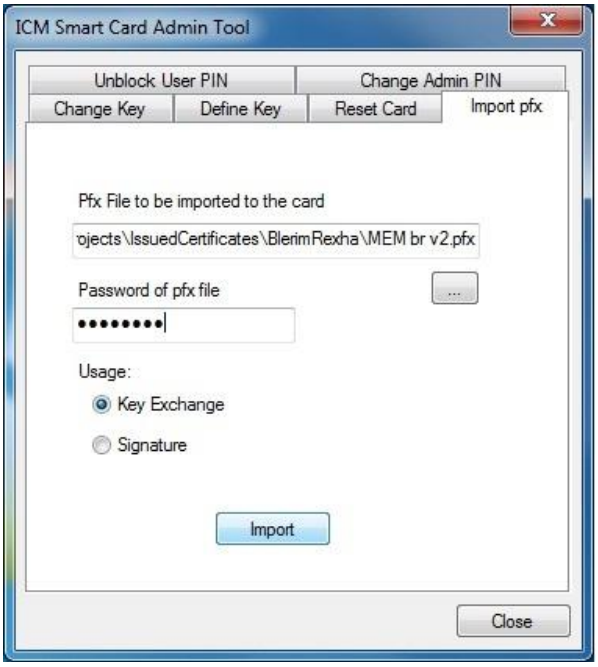


Fig. 12: File structure of SICRYPT

Smart cards have proved secure, tamper-resistant and very suitable devices for storing sensitive information such as keys and certificates. Smart cards can process data in an intelligent form by taking different actions based on secret data that never leaves the card. Memory access to smart cards is guarded by PIN and only after successful PIN presentation does the smart card perform security operations. In the case of several false PIN presentations the smart card is blocked for further memory access, thus protecting the information it holds from unauthorized access. Preventing unauthorized access to sensitive information contained on the card is one the most important security features of the smart card. The advantage of smart cards over other cards is that smart cards have a processor which manages access to data storage through the use of a “user secret", the PIN. The ISO 9564-1 standard recommends that PIN length should be between the 4 and 12 digits. A PIN of four digits is becoming widespread but the PIN length primary depends on the application's security requirements. In general smart card security features are guaranteed through software and hardware security mechanisms of the microprocessor. The security mechanisms of the smart card must be satisfied at every step of the smart card life cycle, from the chip manufacturer, card issuer and during usage by the end user [16].

The "ICM Smart Card Admin Tool" tool (software tool from United Access GmbH, a company in Tulln, Austria) is used to import the X.509 certificate and private key into the smart card, as presented in Fig. 13 and Fig. 14.

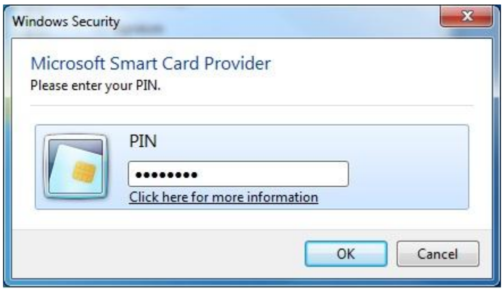


Pfx File to be imported to the card
ojects\IssuedCertificates\BlerimRexha\MEM br v2.pfx

Password of pfx file
••••••••

Usage:
● Key Exchange
○ Signature

Fig. 13: Import certificate into smart card



Windows Security

Microsoft Smart Card Provider

Please enter your PIN.

PIN ••••••••

Fig. 14: PIN verification dialog

The OpenSSL toolkit generates the private and public key, which are stored in a "pem" file format, fully in compliance with [14]. To export certificate and private key from a "pem" file into Public Key Cryptographic Standard number 12 (PKCS#12) format the pkcs12 function of the OpenSSL toolkit is used. This tool supports files of "p12" type, i.e. which have the PKSC#12 format or Microsoft "pfx" file type. PKCS#12 is a standard format for storing private keys and certificates and is used in Netscape and Microsoft Internet Explorer with their import and export options.

5 Conclusion

Shifting the student paper form services towards e-Services and very recently to mobile services (m-Services) is becoming a mandatory feature in a modern university. The approach presented in this paper uses digital X.509 certificates with extended properties in the certificate's subject field. These types of user certificate can be used in any upcoming e–Government services. Smart cards have been proved to be tamper-resistance, secure and reliable devices. The access to a smart card is protected with a PIN known only to the smart card holder. Smart cards are used as secure storage for the private key and its corresponding X.509 digital certificate and as a secure processing device, since encryption with a private key (digital signature) is computed internally in the smart card. Although X.509 certificates have been criticized by [17] for their unique serial number and unique issuer name, which makes them very easy to trace as explained in [18], we will do not concern ourselves here with making anonymous digital signatures. During the six semester testing period, students readily accepted the system. There were a few minor improvements in the software which was brought about from student feedback. The crowd of students at the administration office was reduced to a minimum (almost none), students had more time to study and administrative staff had more time to improve their services. It is worth stressing that none of the administrative staff will be dismissed from their jobs as a result of implementing the SLMS, to the contrary, they will be able to offer with more efficient ways of providing services to students and faculty management. As a result of these many potential benefits, the University of Prishtina is considering to extend this application to all its faculty units.

References:

[1] University of Prishtina, http://web.uni-pr.edu/repository/docs/Statute_of_the_University.pdf link visited at January 2010

[2] University of Prishtina, Official report for the academic year 2007/08, http://web.uni-pr.edu/repository/docs/pasqyra_up_2008.pdf link visited at January 2010

[3] Blerim Rexha, Haxhi Lajqi and Myzafere Limani, Using Smart Cards and X.509 Digital Certificates for a Student Management Information System at the University of Prishtina, the 4th WSEAS European Computing Conference (ECC'10), Bucharest, Romania, April 20-22, 2010

[4] Ian Sommerville, Software Engineering, 8th Edition, Edition Addison-Wesley Publishers Limited, , ISBN = 978-0-321-31379-9, pp. 247, 2007

[5] Hyungrim Choi, Changsup Lee, Yongsung Park, Jaehyung Cho, Taewoo Kwon, Design of Life Cycle Management System of Logistics Information Standards and its Realization, Proceedings of the 3rd International Conference on Communications and Information Technology (CIT'09) Vouliagmeni, Athens, Greece, December 29-31, 2009

[6] Blerim Rexha, Bedri Dragusha and Ilir Limani, Feed-in Tariffs in Kosovo, the 5th IASME / WSEAS International Conference on Energy and Environment (EE'10) Cambridge, UK, February 23-25, 2010

[7] Ronald L Rivest. Cryptography, Chapter 13 of Handbook of Theoretical Computer Science, (ed. J. Van Leeuwen) vol. 1. MIT Press, ISBN =0262720140, 1994.

[8] Hans Delf and Helmut Knebl. Introduction to Cryptography Principles and Applications.

Springer Verlag Berlin Heidelberg, ISBN = 3-540-42278-1, 2002.

[9] Cristea Boboila and Nicolae Constantinescu, CELICA: A Multi-Agent Communication System for Electronic Commerce, Proceedings of the 4th WSEAS European Computing Conference (ECC'10), Bucharest, Romania, April 20-22, 2010

[10] Shivaram H. Mysore, Windows Vista Smart Card Infrastructure, Microsoft Press, August 2007

[11] Bruce Schneier. Applied cryptography: protocols, algorithm, and source code in C. John Willey & Sons, Inc, ISBN = 0-471-12845-7, 1996.

[12] OpenSSL Project, http://www.openssl.org/, link visited at Mai 2010

[13] Blerim Rexha, Ehat Qerimi, Valon Raça and Haxhi Lajqi, Building governmental Certification Authority using OpenSSL – FLOSSK'09, International Conference for Open and Free Software, Prishtina, Kosovo, August 2009

[14] D. Cooper, S. Santesson, S. Farrell, S. Boeyen and W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Network Working Group Request for Comments: 5280, http://tools.ietf.org/html/rfc5280, visited at Mai 2010

[15] Infineon Chip Card and Security ICs Portfolio Proven security you can trust, http://www.infineon.com, visited at Mai 2010

[16] Wolfgang Rankl und Wolfgang Effing, Handbuch der Chipkarten, 5. Auflage, Carl Hanser Verlag München Wien ISBN: 978-3-446-40402-1, 2008

[17] Stefan A Brands. Rethinking Public Key Infrastructure and Digital Certificates, Building, MIT Press, ISBN= 978-0262024914, 2000.

[18] Mattew MacDonald and Erik Johansson, C# Data Security Practical .NET Cryptography Handbook. Wrox Press Ltd. UK, ISBN = 1-86100-801-5, 2003.