Using Smart Cards and X.509 Digital Certificates for a Student Management Information 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 software solution for the implementation of a Student Management Information System at the University of Prishtina. 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. The issued X.509 digital certificate is used to digitally sign the student grades, which is in full compliance with the Kosovo Law on Information Society. For security reasons, the certificate and its associated private are stored in a smart card. The access to private key is protected by a personal identification number. The protection of the student grades against misuse was a “must have” feature of the software solution for the management of the university. This implementation was installed at the Faculty of Electrical and Computer Engineering and has successfully passed a six semester testing period. Beyond increasing the security of the systems, students were, for the first time in the history of the University of Prishtina, able to apply online to take an exam.

Key-Words: - Digital Signature, Privacy, Security, Smart Cards, X.509 Digital Certificates

1 Introduction
The University of Prishtina is the only public university in Kosovo. It 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 [1].

<table>
<thead>
<tr>
<th>Students</th>
<th>Teachers</th>
<th>Administrative staff</th>
<th>Academic Unit</th>
<th>Courses</th>
<th>Exams/Year</th>
<th>Graduated students/Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.318</td>
<td>1.055</td>
<td>61</td>
<td>17</td>
<td>2500</td>
<td>10</td>
<td>1500</td>
</tr>
</tbody>
</table>

One of the main challenges of the university’s management is the poor services 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 management system. Paper records can be lost, duplicated and 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.

2 The Paper Form Procedures
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 signed 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, who in turn have to copy by hand the grade into the main faculty book and save this from the paper form to a paper student file [2]. 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. 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. The student file saved only in the paper form presents a weak point of student management information system.

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, such as digital signature for assuring data security and the applying for an exam via the Internet.

3 Shifting to Digital Signature and the Internet
3.1 Application architecture
The University of Prishtina has its university network in place, i.e. all faculty units are connected over the Local Area Network (LAN) with central administration. In the Fig. 1 is presented the general architecture of the Student Management Information System (SMIS) software solution. This solution was implemented by a local software company in Prishtina. The SMIS was developed with three tier architecture, whereby the Microsoft SQL Server was used as database management system and Microsoft’s Internet Information Service (IIS) as application server [3]. The SMIS, as is depicted in Fig.1, has two views: (i) the Windows form (application) – which is used by the faculty staff to manage the teaching courses and inserting student grades into the system, and (ii) the 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.

3.2 Windows application and smart cards
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 [4]. The application was installed in each client computer, i.e. faculty staff: lecturers and administrative clerks. Each lecturer has received a digital X.509 certificate issued by a local Certification...
Authority (CA) trust center in Prishtina. The X.509 certificate is generated by OpenSSL software. This certificate, including the associated private key, was stored in a smart card. The access to the private key stored in the smart card is protected by a Personal Identification Number (PIN). After issuing the smart card with an installed certificate to lecturers, they are enforced by software policy to change the initial PIN of the smart card. As the smart card is used Infineon SICRYPT card [5]. The X.509 digital certificate includes beyond the standard properties also the Citizen Identification Number (CIN) from Kosovo Civil Registry (KCR) within subject’s name, as is presented in Fig. 2.

Fig. 2: Using X.509 digital certificate for grade signing

In order for the lecturer to protect student grades from misuse, he has to digitally sign each student exam grade (same step as in paper form, signing with handwritten signature). The novelty of this approach is that the CIN is used in the X.509 certificate in the subject’s Common Name (CN) properties, as presented in Fig. 2. A custom batch file was developed to include this feature in OpenSSL software [6]. Therefore this X.509 certificate can be used in all upcoming e-Government services, where CIN is required such as bank transactions, tax refunds, civil registry etc.

3.3 Web application
The web application was developed using C# and Active Server Pages (ASP) as programming language, and the latest Microsoft .NET runtime. The whole communication between user browser and web server is encrypted by SSL. This application is used only by students. During the first semester period, each student is assigned with a fix username and a dynamic temporary initial password that that must be changed at the first login. Changing of the initial password is enforced by security policy. The username is the faculty student ID, and the initial password consists of the faculty student ID plus the concatenated string of student birthdate. This method has until now, shown no cases of student accounts abuse. In SMIS database is stored only the salted hash of the student password, so no one can retrieve and misuse user passwords. Secure Hash Algorithm v1 (SHA1) is used as hash algorithm. Through this application, a student will be able to apply for an exam, receive the exam results and see his student file over the Internet, as is presented in Figure 3.
3.4 Assuring data security

The four main requirements of data security: (i) confidentiality, (ii) integrity, (iii) authentication, and (iv) non-repudiation are achieved through using state of the art encryption techniques and applying the digital signature over sensitive data [4]. The user access 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 clerks who can access only administrative data,
- Lecturer – teaching staff of the faculty, who can access only their respective teaching data and each possess a X.509 digital certificate, smart card and smart card reader,
- Management – faculty management (dean and vice deans) who can create lot of management statistics about the faculty.

One of the main requirements of the SMIS 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 authorized form. Therefore, **protection to this very popular attack is the approach that each student grade is digitally signed by the lecturer private key stored in a smart card**, as presented in Fig. 4.

If by any case an unauthorized user grants access to the database server, he can not insert any new record into the database because he does not possess the private key needed for the digital signature. This private key, as mentioned earlier, is stored only in the smart card of the lecturer. The private key never leaves the smartcard and it can be used for digital signature only after successful personal identification number presentation. However, what an unauthorized user can do is to forge the student grade. The SMIS is protected against this data inconsistency in the following way: the faculty clerk 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. 5. In this form the entire responsibility lies with the lecturer, 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 in our case.
4 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. Although X.509 certificates have been criticized by [5] for their unique serial number and unique issuer name, which makes them very easy to trace [6], 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 SMIS, 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 Pristina is considering to extend this approach to all faculty units.

References: