Construction of Graduation Certificate Issuing System Based on Digital Signature Technique

Assist. Prof .Dr. Mohammed Issam Younis
Department of Computer Engineering
College of Engineering / University of Baghdad
younismi@coeng.uobaghdad.edu.iq

Assist. Lect. Hayder Faez Abdulkareem
Department of Computer Engineering
College of Engineering / University of Baghdad
haiderfaiz@ yahoo.com

Assist. Prof. Hamid Mohammed Ali
Department of Computer Engineering
College of Engineering / University of Baghdad
habdul_hussain@yahoo.com

ABSTRACT

With the development of computer architecture and its technologies in recent years, applications like e-commerce, e-government, e-governance and e-finance are widely used, and they act as active research areas. In addition, in order to increase the quality and quantity of the ordinary everyday transactions, it is desired to migrate from the paper-based environment to a digital-based computerized environment. Such migration increases efficiency, saves time, eliminates paperwork, increases safety and reduces the cost in an organization. Digital signatures are playing an essential role in many electronic and automatic based systems and facilitate this migration. The digital signatures are used to provide many services and solutions that would not have been possible by the conventional hand-written signature.

In the educational environment, the process of issuing the graduation certificates can no longer be restricted to the traditional methods. Hence, a computerized system for issuing certificates of graduation in an electronic form is needed and desired. This paper proposes a Graduation Certificates Issuing System (GCIS) based on digital signature technology. In doing so, this research highlights the state-of-the-art and the art-of-the-practice for some existing digital signature-based systems in the literatures. In addition, eight intertwined elected services are identified, namely: message authentication, entity authentication, integrity, non-repudiation, time stamping, distinguished signing authorities, delegating signing capability and supporting workflow systems. Moreover, this research examines nine existing systems, showing their merits and demerits in terms of these elected services. Furthermore, the research describes the architectural design using the Unified Modeling Language (UML) and provides the concrete implementation of the proposed GCIS. The GCIS is implemented using Visual Basic.Net programming language and SQL Server database management system.

Keywords: Digital Signature, Graduation Certificates Issuing System, Unified Modeling Language.

بناء نظام لإصدار وثيقة التخرج بالاعتماد على تقانة التوقيع الرقمي

د. محمد عصام يونس
قسم هندسة الحاسبات
كلية الهندسة / جامعة بغداد

م.م. حيدر فائز عبد الكريم
قسم هندسة الحاسبات
كلية الهندسة / جامعة بغداد

أ. م. حامد محمد علي
قسم هندسة الحاسبات
كلية الهندسة / جامعة بغداد

الخلاصة

مع التطور العلمي الهائل لمعمارية الحاسوب وتقاناتها في السنوات الأخيرة، أصبحت التطبيقات مثل التجارة الإلكترونية، الحكومة الإلكترونية، الحوكمة الإلكترونية، والتمويل الإلكتروني منطقة للبحث العلمي النشط على نطاق واسع. وبالنتيجة أصبح لزاما الهجرة من البيئة الورقية إلى البيئة المحوسبة المستندة إلى الرقمية من أجل زيادة جودة وكمية المعاملات اليومية المنجزة. هذه الهجرة تزيد من الكفاءة، وتوفر الوقت، وتلغي المعاملات الورقية، وترفع درجة الأمان، وتقلل من التكلفة في المؤسسة. ومما يجدر الاشارة اليه أن التوقيعات الرقمية تلعب دورا أساسيا في العديد من الأنظمة الإلكترونية وتسهل هذه الهجرة. تستخدم التوقيعات الرقمية كوسيلة لتوفير العديد من الخدمات والحلول والتي من غير الممكن تحقيقها بواسطة التوقيعات اليدوية التقليدية.

إن عملية إصدار وثائق (شهادات) التخرج لا يمكن أن تبقى مقتصرة على الطرق التقليدية في البيئة التعليمية. وبالتالي، أصبح لزاما توفير نظام محوسب لإصدار وثائق التخرج في شكل الكتروني. على هذا النحو، يقترح هذه البحث بناء نظام لإصدار وثائق التخرج (GCIS) بالاعتماد على تقانة التوقيع الرقمي. وبالقيام بذلك، يتبنى هذا البحث تسليط الضوء على حالة بعض الأنظمة المستندة على التوقيع الرقمي وواقعها العملي. فضلا عن ذلك، يحدد هذا البحث ثمانية خدمات منتخبة ومتشابكة، هي: مصادقة الرسالة، مصادقة الكيان، النزاهة، عدم التنصل، ختم الوقت، سلطة التوقيع الجزئية (التوقيع حسب الصلاحية او المسؤولية)، وتفويض القدرة على التوقيع (التخويل بالتوقيع)، ودعم نظم سير العمل. وعلاوة على ذلك ، يسلط هذا البحث الضوء على تسعة من النظم القائمة ، ويبين مزايا وعيوب كل منها بالاعتماد على الخدمات المنتخبة الآنفة الذكر. أخيرا، يصف البحث التصميم المعماري باستخدام لغة النمذجة الموحدة (UML) وتوفر التنفيذ الملموس للنظام المقترح. ومن الجدير بالذكر، إن النظام المقترح تم تنفيذه باستخدام لغة البرمجة (Visual Basic.NET) ونظام إدارة قواعد البيانات (SQL Server).

الكلمات الرئيسية : التوقيع الرقمي، نظام إصدار وثائق التخرج، لغة النمذجة الموحدة.

1. INTRODUCTION

Organizations have been trying to move from a paper-intensive environment to a paper-free environment. Word processors have replaced the writing pad and pen, spreadsheet applications have replaced manual spreadsheets, and e-mails have supplanted handwritten letters. Organizations are moving away from the traditional, time consuming paper processes and searching for new and innovative technology to improve efficiency **,Zupan, 2006.** As digital technologies continue to develop rapidly, this impact on many daily tasks which rely on technology. Many of the paper-based documents are being gradually replaced by their electronic versions, such as e-Tickets, e-mail, online (internet) banking and e-Portfolios. These technologies are powerful, flexible and bring huge advantages **,Chen-Wilson, et al., 2011.**

Nowadays various applications such as banking, sale-purchase and stock trading are increasing day by day and emphasizing on electronic transaction to minimize the operational cost and

increasing the services. This need has led to the development of the new notion of electronic document that can be generated, processed and stored in computers and transmitted over the net. The information transmitted over these documents can be susceptible and thus need to be protected from intruders and malicious third parties. Traditionally, in paper document this kind of protection is provided by the written signature and thus it authenticates the document for the communicating parties. For electronic documents, this facility is provided by means of digital signature. Using the digital signature algorithms can provide authenticity and validation to the electronic document **,Shukla, et al., 2012.** With the development of computer engineering and technology, e-commerce, e-government and e-finance are widely used. Digital signatures are playing an important role in many electronic and automatic based applications **,Wang and He, 2010.** Therefore, the migration from the paper-based systems to the electronic or digital-based systems emphasizes the need for the digital signature **,Fazlagic, 2010.**

Digital signatures can significantly benefit organizations by eliminating the last of the paper in the business cycle. The ability to instantly sign and seal documents and transactions electronically results in much shorter process cycle times, accelerated customer service and drastic cost savings. Digital signatures provide enhanced convenience for both the customer and the organization, while significantly reducing application processing time **,Zupan, 2006.**

The remainder of this paper is organized as follows: Section 2 highlights literature review. In addition, this section presents the problem statements and the motivation of this research work. Section 3 presents the additional elected services that must be provided by the digital signature beside the basic services. Section 4 gives the art-of-the-practice of related works. Section 5 gives the architectural design of the proposed system. Section 6 discusses the implementation issues. Section 7 gives a comparison of the proposed system against the existing works. Section 8 gives the conclusion. Finally, Section 9 gives recommendations for future works.

2. LITERATURE REVIEW

Since the introduction of the concept of "digital signature" by Diffie and Hellman in their classic paper "New Directions in Cryptography" **,Diffie, and Hellman, 1976.** this subject has been widely studied and employed in different systems. This section briefly describes the major developments.

- Josang A. and AlFayyadh B. **,Josang, and AlFayyadh, 2008.** proposed a method for WYSIWYS (What You See Is What You Sign) that ensures the integrity of digital documents and their digital signatures. This method can only be directly applied to documents written with traditional American Standard Code for Information Interchange (ASCII) characters. The WYSIWYS property articulates that the bit representation of digital documents must be visualized consistently and as intended to the signer by the digital signature system.
- Zefferer T. and Knall T. **,Zefferer, and Knall, 2010.** introduced a circular Resolution Database System (RDS). The circular RDS is based on the Austrian citizen card concept and makes use of qualified electronic signatures that provide means for secure authentication of users as well as for electronic signing of digital documents.

- Kang B. and Han J. **,Kang , and Han, 2010.** proposed a Threshold Proxy Signature Scheme (TPSS). The TPSS uses a warrant, which is agreed and signed by the original signer and all proxy signers together. In a proxy signature scheme, the original signer is allowed to authorize a designated person as his/her proxy signer, and then the proxy signer is able to sign on behalf of the original signer.
- Fazlagic S. **,Fazlagic, 2010.** proposed a Delegating Digital Signing Capability Mechanism (DDSCM) during a workflow process taking into account the need for verification of digital signature and document integrity after a document is archived.
- Zhou Y. et al. **,Zhou, et al., 2010.** proposed a Threshold Signature Scheme (TSS) with distinguished signing authorities. The proposed scheme not only has the property of threshold signature generation, but also has the property of threshold signature verification. Furthermore, the proposed scheme is a group oriented signature scheme with distinguished signing authorities, in which the signers do not have to sign the whole documents but only a part of the document.
- Liu Z. et al. **,Liu, et al., 2011.** proposed a Multi-Proxy Signature Scheme (MPSS) with proxy revocation. The MPSSs are very useful tools when an original signer needs to delegate his/her signing capability to a group of proxy signers. The proxy revocation means the revocation of delegated rights for the situation where proxy signer or signer's key is compromised and the delegated rights are abused. It may also happen that the original signer wants to terminate the delegated rights before the expiration of the delegation period.
- Chen T. and Lin F. Y. S. **,Chen , and Lin, 2011.** proposed an Electronic Medical Record (EMR) system with a re-signing scheme which is used to make a going-expired digital signature been resigned in time, in keeping with the premise of not conflicting with the laws, morals and privacy while maintaining the security of the EMR system.
- Feng W. et al. **,Feng, et al., 2011.** proposed a Multi-Policy Threshold Signature Scheme (MPTSS) with distinguished signing authorities. In this scheme two groups can sign and verify each other, so the scheme is two-way signing and verifying. Moreover, the threshold values of the two groups can change with the security classification of the signing document and every discretionary signatory only signs a small part of the document instead of the whole one.
- Zhang L. et al. **,Zhang, et al., 2012.** proposed a provably secure Certificateless Proxy Signature Scheme (CLPSS). A proxy signature scheme allows a proxy signer to sign messages on behalf of an original signer within a given context. The Certificateless Public key Cryptography (CL-PKC) has the advantages of no certificate management and no key escrow compared with traditional public key cryptography and identity-based public key cryptography respectively.

2.1 Problem Statements And Motivation

The processes of issuing the various documents are still in a paper form and have been done in a manually and routinely manner that does not fit with the technological progress and the current age requirements and variations. Moreover, using paper-based systems is a costly

process and causes waste of precious time including the possibility of damaging and losing of paper documents. Furthermore, the archiving process for the increasing stacks of document papers would become very difficult to look after or sort out. The switching from paper based work to a fully computerized work is not without difficulties. As a result, many systems have been developed in the recent years. Eight intertwined elected services will be identified; namely: message authentication, entity authentication, integrity, non-repudiation, time stamping, distinguished signing authorities, delegating signing capability and supporting workflow systems. Useful works have been done in the literature as reviewed in the previous section. However, these systems are missing a number of services. Moreover, the combination of all the elected services is missing in the benchmarked systems. This combination is a challenging process that stresses the need of a computerized workflow. Motivated by such challenge, this research aims to solve the manual work problems and provide the combination of the elected digital signature services mentioned before by adopting a system for issuing the graduation certificates in the educational environment.

3. DIGITAL SIGNATURE SERVICES

Digital signature services include message authentication, message integrity, non-repudiation and message confidentiality. A digital signature can directly provide the first three; for message confidentiality it is still a need for using encryption/decryption techniques. Also, a digital signature scheme can provide the entity authentication. However, ordinary digital signature schemes are not quite enough to satisfy some practical needs **,Hwang, et al., 2013.** Thus, there are other services related to digital signature include time stamping, distinguished signing authorities, delegating signing capability and supporting workflow systems.

3.1 Message Authentication

A digital signature scheme can provide message authentication (also referred to as data-origin authentication). Bob can verify that the message is sent by Alice because Alice's public key is used in verification. Alice's public key cannot verify the signature signed by Eve's private key **,Forouzan, 2010.** Digital signatures can be used to authenticate the source of documents or messages (i.e., authentication of a device, a message sent by the device and/or a person sending the message); by creating a digital signature of a message using the private key, which can be verified using the public key. The relationship of a public key to a user's private key allows a recipient to authenticate and validate a sender's message. As ownership of secret key(s) is bound to specific users, valid signatures guarantee that a document was signed by that user **,Ahmed, et al., 2012. ,Singh, et al., 2012.**

3.2 Entity Authentication (Identification)

Entity authentication is a technique designed to let one party prove the identity of another party. An entity can be a person, a process, a client or a server. The entity whose identity needs to be proven is called the claimant; the party that tries to prove the identity of the claimant is called the verifier. Entity authentication is required when Alice gets cash from an automatic teller machine. Entity authentication happens in real time and authenticates the claimant for the entire duration of the session **,Forouzan, 2008.**

Entity authentication is the security process that validates the identity of the communicating party. In the simplest implementation, this takes the form of a password **,Banday, 2011.** The use of a password is the simplest and oldest method of entity authentication. In password authentication, the claimant proves his/her identity by demonstrating that he/she knows a secret, the password **,Forouzan, 2008.** Entity authentication can also be achieved using a digital signature. When a digital signature is used for entity authentication, the claimant uses his/her private key for signing and the verifier must use the public key of the claimant for the purpose of verification **,Forouzan, 2007.**

3.3 Message Integrity

The integrity of the message is preserved even if the whole message is signed because it is infeasible to get the same signature if the message is changed. The digital signature schemes use a hash function in the signing and verifying algorithms that preserves the integrity of the message **,Forouzan, 2007.** A valid digital signature can assure the recipient the origin and the integrity of a message **,Wu, et al., 2013.**

3.4 Non-repudiation

A trusted third party is used to solve many problems concerning security services. The digital signature with a trusted third party could be used for achieving non-repudiation service **,Wu, et al., 2013.** If in the future Alice denies that she sent the message, the center can show a copy of the saved message. If Bob's message is a duplicate of the message saved at the center, Alice will lose the dispute **,Forouzan, 2007.**

3.5 Time Stamping

One of the major drawbacks of digital signatures is the fact that there is no inherent certainty about date and time at which a document was signed. A signer may have included a time stamp with the signature. The document itself may also have a date mentioned on it. However, later readers cannot be certain the signer did, for example, backdate date and time of the signature. Trusted time stamping in addition to digital signatures is needed to prevent such cases of misuse **,Sageder, et al., 2008.** A time stamping service supports assertions of proof that a datum existed before a particular time. One of the major uses of time stamping is to time stamp a digital signature to prove that the digital signature was created before a given time **,Mir , and Banday, 2012.** In many situations, people need to certify that a document existed on a certain date. Thus, the digital signatures are improved by including the time stamps. In doing so, the date and time of the signature are attached to the message and signed along with the rest of the message **,Schneier, 1996.**

3.6 Distinguished Signing Authorities

For the sake of labor-division and responsibility sharing inherent in certain applications and the group works, every discretionary signatory within the group might be required to sign or read the partial document instead of the whole document **,Feng, et al., 2011.** Under this scenario, the

document is divided into several parts and each signer signs only on the part which he is responsible for where each signer signs a partial document that he is responsible for **,Chien, 2005.** Each group member is responsible for his or her own signing of a partial document or message **,Yoon, and Yoo, 2006.** For example, a company releases a document that may involve the financial department, the marketing department and the program office. Each entity signs the partial message related to his work. Each signer signs the section message that he is responsible for **,Huang, and Chang, 2005.**

3.7 Delegating Signing Capability

In the digital world, the original signer delegates its signing capabilities to another person. For example, a manager can delegate to his staff member the right to sign certain documents during his absence, who can sign documents as a proxy signer on behalf of the manager. In such digital schemes referred to as proxy signature schemes, the original signer is able to delegate his signing capability to a designated person. This concept is referred to as one-to-one proxy signature **,Fazlagic, 2010.** In a proxy signature scheme, an original signer can delegate his or her signing capability to a proxy signer and then the proxy signer can generate a valid signature on behalf of the original signer **,Liu, et al., 2011.** The simplest approach to achieve the main goal of a proxy signature scheme is for the designator (original signer) to give its secret key to the proxy signer, who can then use it to sign messages. In this case proxy signatures are just standard signatures, and can be verified the usual way. This scheme called full delegation in the literature **,Boldyreva, et al., 2012.**

3.8 Supporting Workflow Systems

Nowadays, information systems must be able to deal with a highly dynamic environment. Traditionally, workflow systems have been used by business organizations to support the execution of business processes. In workflow literature each business process can be separated into a set of well-defined and inter-related tasks. By controlling task execution the workflow system ensures sequential signing. Using this workflow functionality along with digital signature schemes provides a mechanism for multiuser document signing. Usually, definition of the workflow process predefines the order of signing the documents. Workflow systems must be able to handle digital signatures for different purposes. For example, workflow processes frequently need multiple signers to sign the same electronic document, in line with the organizational structure. Digital signature scheme also should support document verification during and after workflow process execution **,Fazlagic, 2010.**

4. RELATED WORK IN PRACTICE

This section gives the art-of-the-practice of the up-to-date digital signature-based systems. The following subsections contain a brief description of the components and features of these systems according to the elected digital signature services, namely: the message authentication, the entity authentication, the integrity, the non-repudiation, the time stamping, the distinguished signing authorities, the delegating signing capability and the supporting of workflow systems

services.

4.1 Features of the What You See Is What You Sign (WYSIWYS) System

Based on the elected services, the WYSIWYS system provides the message authentication, the entity authentication, the integrity and the non-repudiation services. However, WYSIWYS does not support the time stamping, the distinguished signing authorities, the delegating signing capability and the workflow systems services **,Josang, and AlFayyadh, 2008.**

4.2 Features of the Circular Resolution Database System (RDS)

The circular RDS comprises features to create, publish and maintain electronic documents. The main objective of this system is to increase the security of basic operations like user authentication and the signing of digital documents. The circular RDS solution incorporates qualified electronic signatures for two purposes. On the one hand, the application of qualified electronic signatures is used to unambiguously and securely authenticate users by means of a citizen card based two-factor authentication. On the other hand, created and maintained resolutions are electronically signed in order to guarantee integrity and non-repudiation of the particular data **,Zefferer, and Knall, 2010.** In addition, the entity authentication is supported in this system. The workflow service being one of the core components of the entire RDS is responsible for all tasks concerning the creation, signing and publishing of resolutions. However, the time stamping, the distinguished signing authorities and the delegating signing capability are not supported in this system.

4.3 Features of the Threshold Proxy Signature Scheme (TPSS)

The TPSS is a (t; n) threshold proxy signature scheme. In a (t; n) threshold proxy signature scheme, the original signer can authorize (n) members of a proxy group. Moreover, only the cooperation of (t) or more proxy members is allowed to generate the proxy signature. In the TPSS, a warrant agreed and signed by the original signer and all proxy signers together has been used. The computation complexity and communication cost of the scheme have nothing to do with the size of the proxy group. Moreover, the verification of proxy signature is divided into two steps, one is the verification of the warrant; the other is the verification of the proxy signature. Having these properties, the proposed TPSS has less computation and communication cost, compared with previously proposed schemes based on discrete logarithms. It is more efficient and secure scheme **,Kang, and Han, 2010.** The TPSS ensures the message authentication, the entity authentication (identities of the original signer and the proxy signers), the integrity of the massage, the non-repudiation and the delegating signing capability services. However, the TPSS does not support the time stamping, the distinguished signing authorities and workflow systems services.

4.4 Features of the Delegating Digital Signing Capability Mechanism (DDSCM) in Workflow Systems

The dynamic nature of business processes imposes the need for the workflow management system (WfMS) to be able to modify a process model at run-time to deal with exceptional

situations and adjust to the changing business policies. A fully computerized workflow processes with a digital signature technology used to provide authenticity and the integrity of electronic documents throughout the document life cycle. The delegating digital signing capability service is achieved by using an appropriate proxy scheme integrated with the WfMS **,Fazlagic, 2010.** Furthermore, the time stamping and non-repudiation services are supported in this system. However, the service of distinguished signing authorities is not supported in this system.

4.5 Features of the Threshold Signature Scheme (TSS) with Distinguished Signing Authorities

In most signature schemes, the signer and the verifier of a signature may be a single person. However, when one message is exchanged between one organization and another organization, the message may require the approval or consent of several members. Under this scenario, the signature generation and verification require more than one consenting rather than by a single member. Threshold signature schemes are introduced to solve this problem **,Zhou, et al., 2010.** Based on elected services, the TSS with distinguished signing authorities provides the message authentication, the entity authentication, the integrity and the non-repudiation services. However, it does not support the time stamping, the delegating signing capability and the workflow systems services.

4.6 Features of the Multi-Proxy Signature Scheme (MPSS) with Proxy Revocation

In some cases, the original signer may delegate his or her signing power to a specified proxy group while ensuring individual accountability of each participant signer. The proxy signature scheme that achieves such purpose is called MPSS, and the signature generated by the specified proxy group is called multi-proxy signature for the original signer. The proxy revocation, i.e., the revocation of delegated rights is needed and it is important for the situation where proxy signer or signer's key is compromised and the delegated rights are abused **,Liu, et al., 2011.** The MPSS satisfies the message authentication, the entity authentication (the original signer and the proxy signers' identities), the integrity of the massage, the non-repudiation and the delegating signing capability services. However, MPSS does not support the time stamping, the distinguished signing authorities and workflow systems services.

4.7 Features of the Electronic Medical Record (EMR) System

The EMR is a digital format of the traditionally paper-based anamnesis (patient's record), which contains the complete medical case history of a patient such as his somewhat illness, current health problems and his chronic treatments. An electronic anamnesis is meant to make the patient's health information more conveniently accessible and transferable between different medical institutions and also easier to be kept quite a long time. In regard to the security purpose, all the EMRs are embedded with both of the PKI cryptography and the digital signature technique so as to ensure the records well-protected **,Chen, and Lin, 2011.** The digital signature that integrated to the EMRs system ensures the authentication, the data integrity and help to verify the non-repudiation of the content. In addition, the time stamping technique is supported in this system. However, the distinguished signing authorities, the delegating signing capability and the workflow systems services are not supported in this

system.

4.8 Features of the Multi-Policy Threshold Signature Scheme (MPTSS) with Distinguished Signing Authorities

There are three trusted parties involved in the MPTSS: the system authority (SA), the document dispatcher (DD) and the signature collector (SC). SA is responsible for defining system public parameters and generating the private keys and the public keys for signing and verifying groups and their members. The tasks of DD are to divide the signing document into smaller subdocuments according to the significance of the document and choose the signatories within the signing group for signing these subdocuments. The responsibilities of SC are to collect and verify individual signatures generated by the signatories, to check whether the contents of the whole document have been signed by these discretionary signatories, and to construct a group signature from the individual signatures **,Feng, et al., 2011.** The MPTSS with distinguished signing authorities provides the message authentication, the entity authentication, the Integrity and the non-repudiation services. However, it does not support the time stamping, the delegating signing capability and the workflow systems services.

4.9 Features of the Certificateless Proxy Signature Scheme (CLPSS)

CL-PKC does not use public key certificates. It successfully solves the key escrow problem. In CL-PKC, a third party called Key Generation Center (KGC) is used to help a user to generate his private key. CL-PKC eliminates the need of certificates and does not suffer from the key escrow problem. Therefore, it is interesting to introduce proxy signatures into CL-PKC. Compared with proxy signature schemes in traditional public cryptography, CLPSS can eliminate the certificate verification and burdensome certificate management. Hence, CLPSS supports true non-repudiation **, Zhang, et al., 2012.** The CLPSS ensures the message authentication, the entity authentication, the Integrity of the massage and the delegating signing capability (proxy signature scheme with delegation by warrant) services but it does not support the time stamping, the distinguished signing authorities and workflow systems services.

5. THE ARCHITECTURAL DESIGN OF THE GRADUATION CERTIFICATES ISSUING SYSTEM (GCIS)

The proposed GCIS performs different functions (activities); these functions are executed by specific users (actors). Therefore, the design of the GCIS will be described by using the UML diagrams to represent the interaction between the actors and the GCIS functions. The UML is a very helpful tool in developing a specific structure according to specific requirements. Based on the elected services related to the digital signature mentioned, the architectural design of the proposed GCIS will be constructed by the use case diagrams.

The use case diagram specifies the functionality that the system has to offer from the perspective of users and defines what should take place inside the system. In addition, this diagram uses "actors" to represent the roles that users can play, and it also utilizes "use cases" to represent what users can do with the system. Thus, the use case diagram consists of two parts **,Al-Tameemi, 2010.**

1. Actor(s): It represents someone or something that acts in the system (i.e., human beings who will interact with the system). The classes of actors capable of using the system are presented in the next section.
2. Use case(s): It is a special sequence of related transactions performed by an actor and the system in a dialogue. The use cases specify all interactions within the system.

Fig. 1 shows the use case diagram of the proposed GCIS and the use cases related to each user.

6. THE IMPLEMENTATION OF THE GCIS

Before going into implementation details, it is necessary to mention that the Visual Studio 2008 (Visual Basic.Net) with the .Net framework 3.5 is used to:

1. Construct the GUIs of the proposed GCIS to allow users to interact with the system.
2. Implement the cryptographic algorithms with regard to the digital signature (RSA digital signature scheme) and the hash function (SHA-512) in addition to the encoding and decoding techniques (UTF-8). It should be mentioned that these cryptographic algorithms are invoked by an industrial standard APIs' built in the "Microsoft .Net" framework.
3. Access and manipulate the data or records stored in the tables of the GCIS within the SQL Server database.

6.1 The Login GUI

The users of the GCIS gain access to the resources of the system through the login GUI. For the purpose of entity authentication (identification) service, each user has a username and password. The users can login by entering a valid username and password as show in **Fig. 2**. The delegated user check box in the login GUI is checked only by the delegated signers for login process, so as distinguishing them from the original signers.

6.2 The Administration GUI

This GUI is used for generating and updating the RSA key pair for the users of the GCIS and to activate the delegating signing capabilities service. **Fig. 3** shows the main administration GUI. The administrators is responsible for accomplishing the tasks related to this GUI.

6.3 The Student's Information GUI

There are two users (with stdinfo1 and stdinfo2 usernames) responsible for inserting (data entry) and updating the main students' information. The GCIS support the share access to the system's resources. In addition, the processes of the system could be performed simultaneously by multi-user due to adopting the client/server paradigm. Therefore, inserting and updating processes could be performed by stdinfo1 and stdinfo2 simultaneously without any conflict. **Fig. 4** shows the data entry mode of the student's information GUI for a certain graduated student.

6.4 The Student's Degrees

There are two users (with stddeg1 and stddeg2 usernames) responsible for inserting and updating the students' degrees. After the login process the student's degrees main GUI will appear which indicates that there are a certain number (between the square brackets) of students' records ready for the inserting and/or updating degrees processes (four students'

records are ready for degrees inserting process in our case study), as shown in **Fig. 5**.

6.5 The Checking Process

When the data entry process of the student's information and degrees records complete successfully then the checkers of the GCIS will be ready for accomplishing the checking processes in order to make sure that there are no mistakes exist in the students' information and degrees records. The checking processes could be done in parallel (i.e., simultaneously) by eight checkers; two checkers for each class. The checkers are responsible for reviewing the student's information, the student's degrees for the subjects, the attempt of each subject and the year related to the specific class. **Fig. 6** shows the details of the checking GUI.

6.6 The Examination Board / Registration Unit Processes

When the checking process is finished successfully for all the graduated students, then several processes should be performed by the examination board/registration unit before issuing the graduation certificates in their final form. **Fig. 7** shows the main examination board/registration unit GUI and the processes related with it. Examination Board / Registration Unit Employees perform the following activities:

1- Automatically, calculating the final averages and the ranks for the graduated students.
2- Editing the syllabus for each class including the subjects' IDs, the subjects' names in English and Arabic languages, and the number of units for each subject.
3- Specifying the types of the required graduation certificates for each student as part of the issuing process. These types include: the certificate of graduation and the transcript of records in Arabic and English languages.
4- Printing the paper copies of the achieved graduation certificates. A soft copy for the finished graduation certificates will be available as a PDF file in addition to the HTML and ASP formats.

6.7 The Final Graduation Certificates Issuing and Signing Processes

After completing the pervious steps, all the required information for issuing the graduation certificates will be available. Therefore, the graduation certificates in their final form will be ready for signing. The signing process will be performed by the following signers (arranged according to the signing process sequence): the examination board member, head of the examination board, head of the department, the registers, the assistant dean, the dean, the issuer (performs the process of inserting the graduation certificate's number and date), and the manager of the higher studies and certifications, respectively.

As in real word, the order of signers should be respected. This fact is taken into account within the internal design of the system. The verification process will be performed automatically for the digital signature of the previous signer. In case of an invalid signature, the signing process will be aborted until fixing the problem. Otherwise, in case of a valid signature, the graduation certificate will appear to the current signer for the reviewing and signing purposes, as shown in **Fig. 8**.

7. COMPARISON OF THE GCIS WITH THE EXISTING DIGITAL SIGNATURE-BASE 1

Table.1 demonstrates the digital signature services of the GCIS compared with the existing systems and schemes.

8. CONCLUSIONS

In this research, a number of existing systems and schemes based on digital signature have been studied in terms of the elected services. Based on that, Graduation Certificates Issuing System (GCIS) has been proposed. The proposed GCIS overcomes the drawbacks in the existing systems and schemes. The proposed GCIS has been implemented by using Visual Studio 2008 (Visual Basic.Net) with .Net framework 3.5, SQL Server 2005 database and Visual Paradigm for UML 8. The proposed GCIS has been compared with the other digital signature based systems. The comparison showed the advantages of the proposed GCIS over the existing systems and schemes. In this paper, the desired elected services have been accomplished as shown below.

8.1 Message Authentication (Data-Origin Authentication) Service

The system provides a message authentication service through the verification processes for the digital signatures of the signers. This service is reflected in the GCIS through employing the cryptographic digital signature algorithms (RSA digital signature scheme). When the user (singer) signs data with digital signature (using his/her private key) someone else (other users) can verify this signature (using the associated signer's public key), and can prove that the data originated from the original user (singer) himself not from other user.

8.2 Entity Authentication (Identification) Service

The system provides the entity authentication service through utilizing the username and password for user (signer). Thus, the identity of each user (signer) will be validated or proven. This service is employed for the purpose of login process in order to gain access to the system’s resources.

8.3 Integrity Service

The system employed the digital signature algorithm for the purpose of signing and verification processes. The digital signature schemes imply the using of the one way hash function to provide the integrity service. Thus, any unauthorized change for the content of the data records will be detected and that will ensure that the received data are exactly as signed by the original signer.

8.4 Non-repudiation Service

Since the system is employing the client/server paradigm, a trusted database server in association with the digital signature technology has been used for providing the non-repudiation service. Thus, the users of the system will not be to deny their activities within the processes of the system.

8.5 Time Stamping Service

The system provides time stamping services through using a stored procedure within the main database to return the current system date and time of the main server. This time stamp will be appended to the data record and digitally signed along with it. Thus, the time stamp service has been accomplished. In addition, the conflicts of the clients' computers time stamps have been avoided.

8.6 Distinguished Signing Authorities Service

The system provides the distinguished signing authorities service for the purpose of labor-division, responsibility sharing, saving efforts and time. This service is exactly reflected in the checking process within the system, in which the student's degrees record has been checked by separated groups of checkers (two checkers for each class). Thus, the signers (checkers) do not have to check and sign the whole student's degrees record but only a part of it.

8.7 Delegating Signing Capability Service

The system provides the delegating signing capability due to changing or absence of the original signer or for any other reason; therefore, another user (signer) will be delegated to sign the final graduation certificates. This service is exactly reflected in the system through filling the delegation form to designate another user (signer) for signing purposes instead of the original signer.

8.8 Supporting Workflow Systems Service

This system is divided into intertwined processes; the execution of each process is dependent on the previous process, which means it could not execute a certain process until completing the process which is related on. This service is reflected in the system, for example the student's degrees inserting process could not be performed until finishing the inserting process of the student's information.

9. REFERENCES

- Ahmed M., Sazzad T. M. S., and Mollah M. E., 2012, "*Cryptography and State-of-the-art Techniques*", International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 2, No. 3., PP. 583-586.

- Al-Tameemi Z. F. A., 2010, "*Design and Implementation of a Scalable Automated RFID Based Attendance System with Scheduling Technique*", M.Sc. Thesis, School of Electrical and Electronic Engineering, University of Science Malaysia, Penang, Malaysia.

- Banday M. T., 2011, "*Easing PAIN with Digital Signatures*", International Journal of Computer Applications (IJCA), Vol. 29, No. 2, PP. 46-56.

- Boldyreva A., Palacio A., and Warinschi B., 2012, "*Secure Proxy Signature Schemes for Delegation of Signing Rights*", Journal of Cryptology, Vol. 25, Issue 1, PP. 57-115.

- Chen T., and Lin F. Y. S., 2011, "*Electronic Medical Archives: A Different Approach to Applying Re-signing Mechanisms to Digital Signatures*", Journal of Medical Systems, Vol. 35, Issue 4, PP. 735-742.

- Chen-Wilson L., Gravell A. M., and Argles D., 2011, "*Giving You back Control of Your Data Digital Signing Practical Issues and the eCert Solution*", Proceedings of the World Congress on Internet Security (WorldCIS) , London, UK , PP. 93-99.

- Chien H., 2005, "*Comments on ID-based Multi-signature with Distinguished Signing Authorities*", Journal of Applied Mathematics and Computation, Vol. 170, Issue 2, PP. 1284-1289.

- Diffie W., and Hellman M. E., 1976, "*New Directions in Cryptography*", Proceedings of the IEEE Transactions on Information Theory, Vol. 22, Issue 6, PP. 644-654.

- Fazlagic S., 2010, "*Delegating Signing Capability in Workflow Systems*", Proceedings of the 2nd IEEE International Conference on Computer Engineering and Technology (ICCET), Chengdu, China, Vol. 4, PP. 324-327.

- Feng W., You-sheng Z., Li-ze G., Shi-hui Z., and Yi-xian Y. , 2011, "*Multi-policy Threshold Signature With Distinguished Signing Authorities*", The Journal of China Universities of Posts and Telecommunications, Vol. 18, Issue 1, PP. 113-120.

- Forouzan B. A., 2008, "*Cryptography and Network Security*", Special Indian Edition, The McGraw-Hill Companies, Inc.

- Forouzan B. A., 2007, "*Data Communications and Networking*", Fourth Edition, The McGraw-Hill Companies, Inc.

- Forouzan B. A., 2010, "*TCP/IP Protocol Suite*", Fourth Edition, The McGraw-Hill Companies, Inc.

- Hwang M., Lee C., and Tzeng S., 2013, " *A New Proxy Signature Scheme for a Specified Group of Verifiers*", Information Sciences, Vol. 227, PP. 102-115.

- Huang H., and Chang C., 2005, "*Multisignatures with Distinguished Signing Authorities for Sequential and Broadcasting Architectures*", Journal of Computer Standards and Interfaces, Vol.27, Issue 2, PP. 169-176.

- Josang A., and Alfayyadh B., 2008, "*Robust WYSIWYS: A Method for Ensuring that What You See Is What You Sign*", Proceedings of the 6th Australasian Information Security Conference (AISC 2008), Wollongong, Australia, PP. 53-58.

- Kang B., and Han J., 2010, "*A More Practical and Efficient Threshold Proxy Signature Scheme*", Proceedings of the 2nd IEEE International Conference on Education Technology and Computer (ICETC), Shanghai, China, Vol. 5, PP. 202-205.

- Liu Z., Hu Y., Zhang X., and Ma H., 2011, "*Provably Secure Multi-proxy Signature Scheme with Revocation in the Standard Model*", Special Issue of Computer Communications on Information and Future Communication Security, Vol. 34, Issue 3, PP. 494-501.

- Mir F. A., and Banday M. T., 2012, "*Authentication of Electronic Records: Limitations of Indian Legal Approach*", Journal of International Commercial Law and Technology, Vol. 7, Issue 3, PP. 223-232.

- Sageder S., Sametinger J., and Wiesauer A., 2008, "*Case Study: Using Digital Signatures for the Archival of Medical Records in Hospitals*", Proceedings of the 3rd IEEE International Conference on Risks and Security of Internet and Systems (CRiSIS'2008), Tozeur, Tunisia, PP. 213-220.

- Schneier B., 1996, "*Applied Cryptography: Protocols, Algorithms, and Source Code in C*", Second Edition, John Wiley & Sons.

- Shukla S., Gupta D. L., and Malviya A. K., 2012, "*A Comparative Study of Cryptosystems with Elliptic Curve Cryptography Using Digital Signature*", International Journal of Computer Technology and Applications (IJCTA), Vol. 3, Issue 1, PP. 9-16.

- Singh K., Kharbanda I., and Kaur N., 2012, "*Security Issues Occur in Cloud Computing and There Solutions*", International Journal on Computer Science and Engineering (IJCSE), Vol. 4, No. 5, PP. 945-949.

- Wang L. and He M., 2010, "*Improved Efficient Forward Secure Signature Scheme*", Proceedings of the IEEE International Conference on E-Business and E-Government (ICEE), Guangzhou, China, PP. 1338-1341.

- Wu W., Zhou J., Xiang Y. and Xu L., 2013, "*How to Achieve Non-Repudiation of Origin with Privacy Protection in Cloud Computing*", Journal of Computer and System Sciences, Vol. 79, Issue 8, PP. 1200-1213.

- Yoon E. and Yoo K., 2006, "*Cryptanalysis of Two Multisignature Schemes with Distinguished Signing Authorities*", Proceedings of the IEEE International Conference on Hybrid Information Technology (ICHIT'06), Cheju Island, South Korea, Vol. 1, PP. 492-495.

- Zefferer T. and Knall T., 2010, "*An Electronic-signature Based Circular Resolution Database System*", Proceedings of the ACM Symposium on Applied Computing (SAC'10), Sierre, Switzerland, PP. 1840-1845.

- Zhang L., Zhang F. and Wu Q., 2012, "*Delegation of Signing Rights Using Certificateless Proxy Signatures*", Information Sciences: an International Journal, Vol. 184, Issue 1, PP. 298-309.

- Zhou Y., Wang F., Xin Y., Luo S., Qing S. and Yang Y., 2010, "*A Novel Threshold Signature Scheme with Distinguished Signing Authorities*", Proceedings of the 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), Beijing, China, PP. 728-732.

- Zupan A., 2006, "*Digital Signature as a Tool to Achieve Competitive Advantage of Organization*", M.Sc. Thesis, Faculty of Economics and International Center for Promotion of Enterprises (ICPE), Ljubljana, University of Ljubljana.

Table 1. Comparison between the proposed GCIS and the related systems.

✓ Implemented service ✗ Not implemented service	Digital signature elected services							
Digital signature-based systems	Message authentication	Entity authentication	Integrity	Non-repudiation	Time stamping	Distinguished signing authorities	Delegating signing capability	Supporting workflow systems

WYSIWYS **(Josang, and AlFayyadh, 2008)**	✓	✓	✓	✓	×	×	×	×
Circular RDS **(Zefferer, and Knall, 2010)**	✓	✓	✓	✓	×	×	×	✓
TPSS **(Kang and Han, 2010)**	✓	✓	✓	✓	×	×	✓	×
DDSCM in Workflow Systems **(Fazlagic, 2010)**	✓	✓	✓	✓	✓	×	✓	✓
TSS with Distinguished Signing Authorities **(Zhou, et al., 2010)**	✓	✓	✓	✓	×	✓	×	×
MPSS with Proxy Revocation **(Liu, et al., 2011)**	✓	✓	✓	✓	×	×	✓	×
EMR System **(Chen and Lin,2011)**	✓	✓	✓	✓	✓	×	×	×
MPTSS with Distinguished Signing Authorities **(Feng, et al., 2011)**	✓	✓	✓	✓	×	✓	×	×
CLPSS **(Zhang, et al., 2012)**	✓	✓	✓	✓	×	×	✓	×
The Proposed GCIS	✓	✓	✓	✓	✓	✓	✓	✓

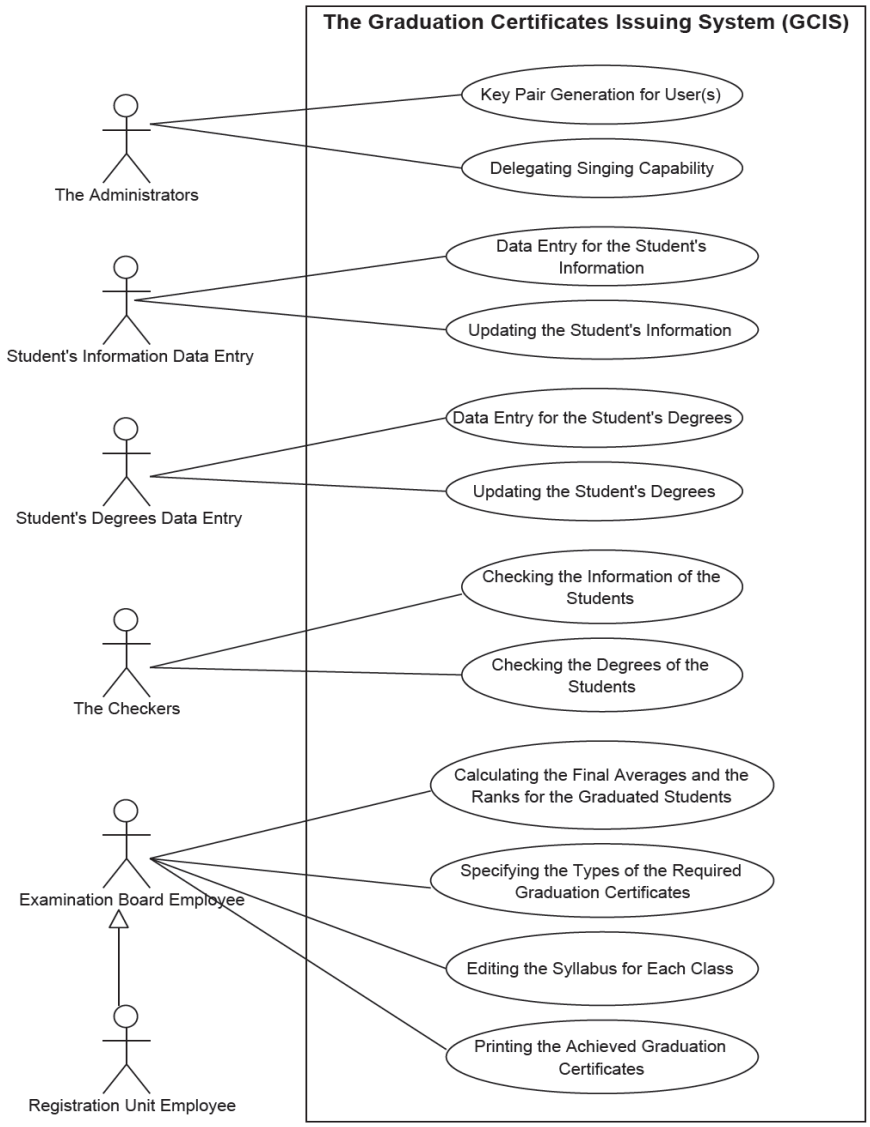

Figure 1. The use case diagram of the GCIS.

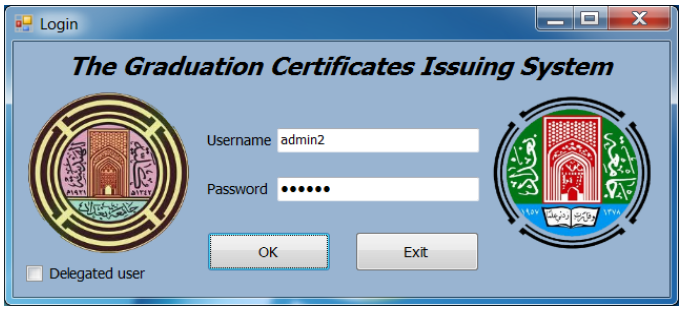

Figure 2. The login GUI of the GCIS.

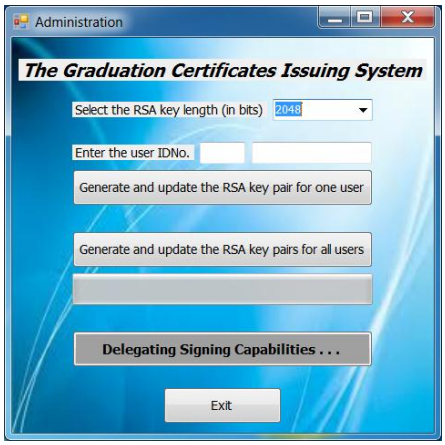

Figure 3. The administration GUI.

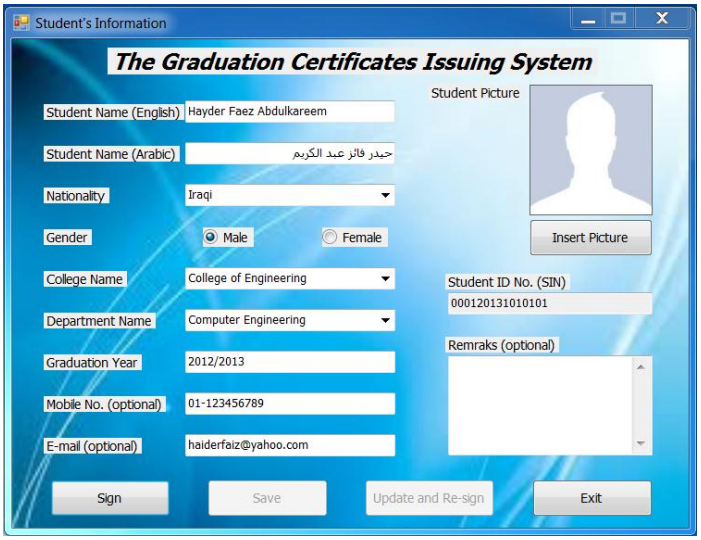

Figure 4 The student's information GUI.

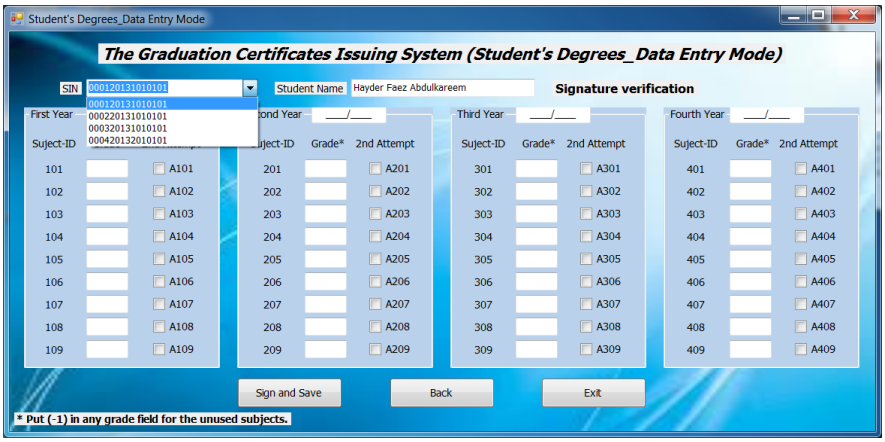

Figure 5. The student's degrees GUI.

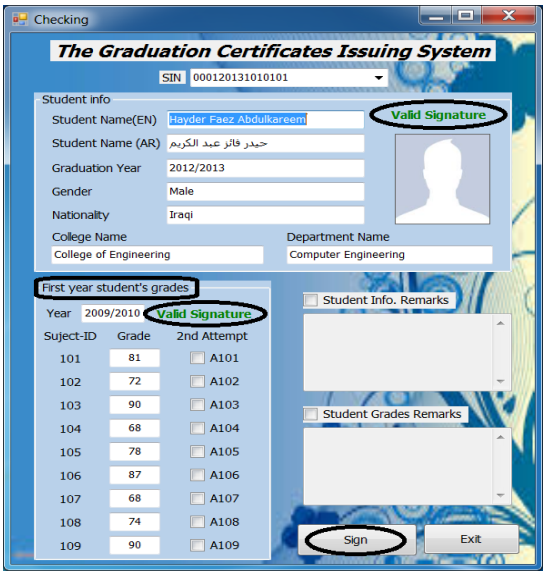

Figure 6. The checking process with valid signatures and no mistakes.

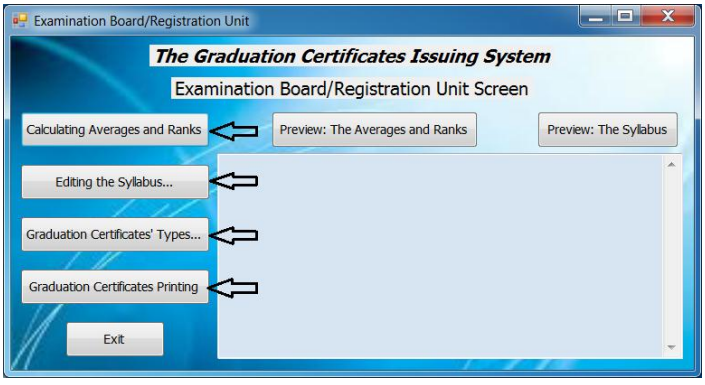

Figure 7. The main examination board/registration unit GUI.

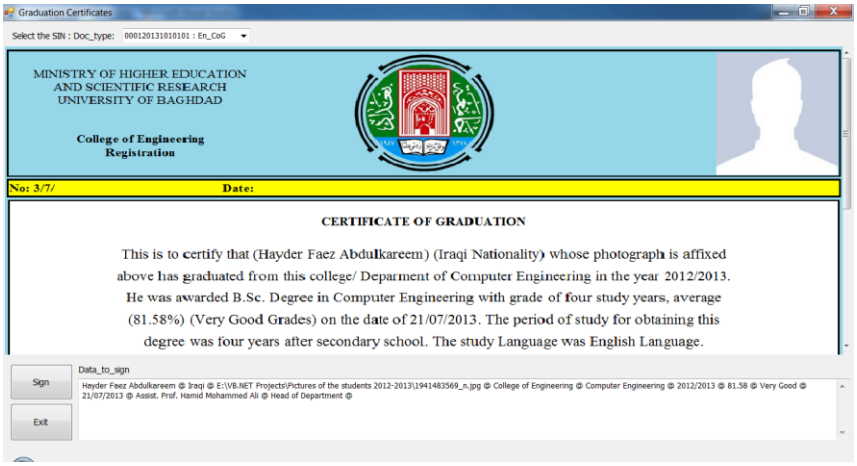

Figure 8. The final graduation certificates issuing and signing GUI.