# Simplify Authentication of Certificates: A Case Study for Directorate of Scholarship and Cultural Relations in Iraq

Maher Hassan Kadhim
*Department of Computer Science*

*Karbala University*

mahir.alsaedi@uokerbala.edu.iq

## Abstract

**Recently, there has been a growing interest in improving the Electronic Government (eGovernment), such as establishing new departments in every ministry and institute to enhance dealing with eGovernment. One example is the use of the Certification Authority of the hyper system. This system is based on using confidential mail and serial numbers of the certificates to test the validity of certification in the chain. The data provided by the user's identity helps in building the equivalence Issuance Certification which reduces the time and cost of automating the authentication process which makes the process simpler to the applicant. It is useful to create a hyper system for certificate authentication to reduce the cost and time of certificate issuance. This paper considers the Directorate of Scholarship and Cultural Relations in Iraq as a case study. In particular, we suggest a method for Certificate equivalence for graduates of overseas universities. Our approach offers a significant improvement in the traditional method used to carry out the certificate authentication process. We aim to pave the way toward using blockchain technology in the field of authentication processes performed by The Iraqi Directorate of scholarship and cultural relations.**

**Keyword**: **Confidential Paper Mail, Web Confidential Issuance Certificates, Iraqi National Identity**



## I. INTRODUCTION

One weakness in the current system for certification authority (CA) is that the information provided by the applicant's certification, such as name, Iraqi National Identity (INI), and serial numbers, are not utilized by the traditional equivalence procedure. The method of utilizing the serial numbers of certificates facilitates the authentication and verification of the certificates authorization procedure chain which has recently been adopted by the majority of the certificate equivalence organizations. (Elwailly, 2004)

In the traditional system, the applicant submits a copy of his documents or just sends them via email. The documents are then reviewed, and if complete, the applicants can find their current status under processing. Otherwise, they may need to submit more documents or update them. (Mohammed et al., 2014) .The applicant can also track his transaction by using new technology that a mobile application provides and that improves the process of the application via Follow App. (Mohammed et al., 2018)

There are many problems with the current system of the governance procedure. First, due to the continuous change in the rules and regulations regarding the certificate equivalence, the metrics of equivalence are amended accordingly. This results in a heterogeneous system that would be very difficult to standardize. Recently, there have been attempts to improve single sign-on (SSO) systems. In these systems, the applicant has a unique certification to access different services provided in a Web-based application form that is easy to fill and interact with (Dong,2016). Furthermore, the implementation of INI in the SSO system helps in improving the quality of the certificates equivalence procedure thanks to the unique number of the INI certificate, which elements duplication and conflicts between documents like full name. The SSO system allows for cooperation aimed at sharing the identity information in a standard, secure, and flexible way .(Elwailly, 2004)

Internet Communication Technology (ICT) has meaningfully affected the way information is given and exchanged. It also changed the way websites are processed, in particular, speeding up processes by resolving geographic and time barriers in our daily lives. Governments have recognized the importance of the Internet to stakeholders such as students who study

overseas, especially for certificate equivalence. "EGovernment", "digital government", "e-democracy", "e-administration", and "e-services" are a sample of the different terms used to explain the same endeavor.

E-government can be defined as a general management program that uses ICT to develop government communication, service, business, and transactional processes with the stakeholders (Kimberly 2004). The service can be initiatives such as connecting internal government departments, uploading information to the public, or responding to citizens' questions and needs (Basu, 2002).

We use the data supplied by the user's identity provider to set his certificate, reducing the costs of maintaining several registration authorities and simplifying the certificate issuance process.

E-government is a massive cost, includes huge risk, requires skilled technical resources, and stable fixed technical infrastructure. The following are especially important in developing e-government: political rootage, passable legal framework, trust in government, stable economic structure, centralized or decentralized government structure, full growth within the government, and citizen requirement. (Basu, 2002).

The Iraqi government has tried to restructure Iraqi states and organizations towards e-government standardization since 2003, and all the subsequent governments have failed to achieve this objective. This is due to the bureaucracy rules the Iraqi republic is built upon. Additionally, there is a lack of planning and development by the US-led coalition for what came after the hostilities of nation-building in Iraq that proved to be poor and unready to commence (Dodge, 2003).

One example of a successful study is *the E-government on NEIS of Korea* in information technology, education fields. The Ministry of Education and Human Resource Development (HRD) completed the construction of the National Education Information System (NEIS). NEIS is a Web-based, integrated and centralized online education administration system and communicates other government bodies to process a one-stop administration service. In spite of almost a secure system, no hacking, no leakage of privacy, a teacher doesn't trust the system. The adoption of IT technology in the education fields has brought about a reduction of redundant administrative works and simplification of complex tasks through automation and standardization of process. General citizens can submit the online requirements for issuance of graduation certificates. (Kim,2006)

After construction NEIS, the teacher encrypts student's information and sent it to correspond to the university. It reduces personal visiting to university and university admission job process. In results, it saved the 10 hours of visiting university per each student. In terms of university, they could cut down 4 steps of a business process in two, 17 days, and 104.8 M USD cost saving. Online request and issuance of certificate reduced time and cost for visiting.

These malformed intermediate certificates were signed by the Government of Korea and provided to educational institutions ranging from elementary schools to universities, libraries, and museums. However, because they are still technically CA certificates, web browsers, including Mozilla Firefox and Google Chrome will not recognize them as valid leaf certificates. The study does not include these certificates when referring to the set of browser-trusted authorities because they are unable to sign any certificates and therefore do not have the same influence as other valid authorities. However, the study notes that some less common client implementations may fail to properly check the path length constraint and incorrectly treat these as valid. One of these CA certificates, issued to a Korean elementary school, was compromised by Heninger, who factored the 512-bit key a few hours after the certificate expired. (Turmeric, 2013)

## *II. THE TRADITIONAL METHOD*

### *A. The traditional certificate equivalence procedure:*

*I. At the applicant's organization or university:*

1. The applicant submits the application with the relevant documents to the department of equivalence at his organization or university.
2. The application is submitted to the dean or chairman.
3. The application is signed by the president's assistant for scientific affairs.
4. The application is signed by the president of the university.

*II. At the Directorate of Scholarship and Cultural Relations (student affairs department):*

1. The application is sent to the Ministry of Higher Education (MOHESR).

2. The application is directed to the Directorate of Scholarship and Cultural Relations in Iraq (SCRDIraq).
3. The application is directed to the students' affairs department.
4. The head of the department directs it to the section the student studied in its state.
5. The section administrator receives the transaction and refers it to the employee "n", then directed according to the type of study.

*III. At the Directorate of Scholarship and Cultural Relations (Equivalence Department):*

1. The employee at this department finishes up the transaction after checking all requirements again in the checklist.
2. The application is referred to the certificate evaluation after making sure all requirements have been met.
3. It is then referred to the section concerned with the scientific specialty (Department of Pure Sciences, Department of Engineering Sciences, Department of Medical Sciences, Department of Administrative Sciences, or Department of Humanities) to determine whether it meets the conditions for equivalence, like a recognized university, subjects and rigor of thesis or dissertation.
4. A certificate is issued by the department and signed by the chairman with an administrative order.
5. The applicant receives the certificate equivalence. This procedure is shown in Figure 1.

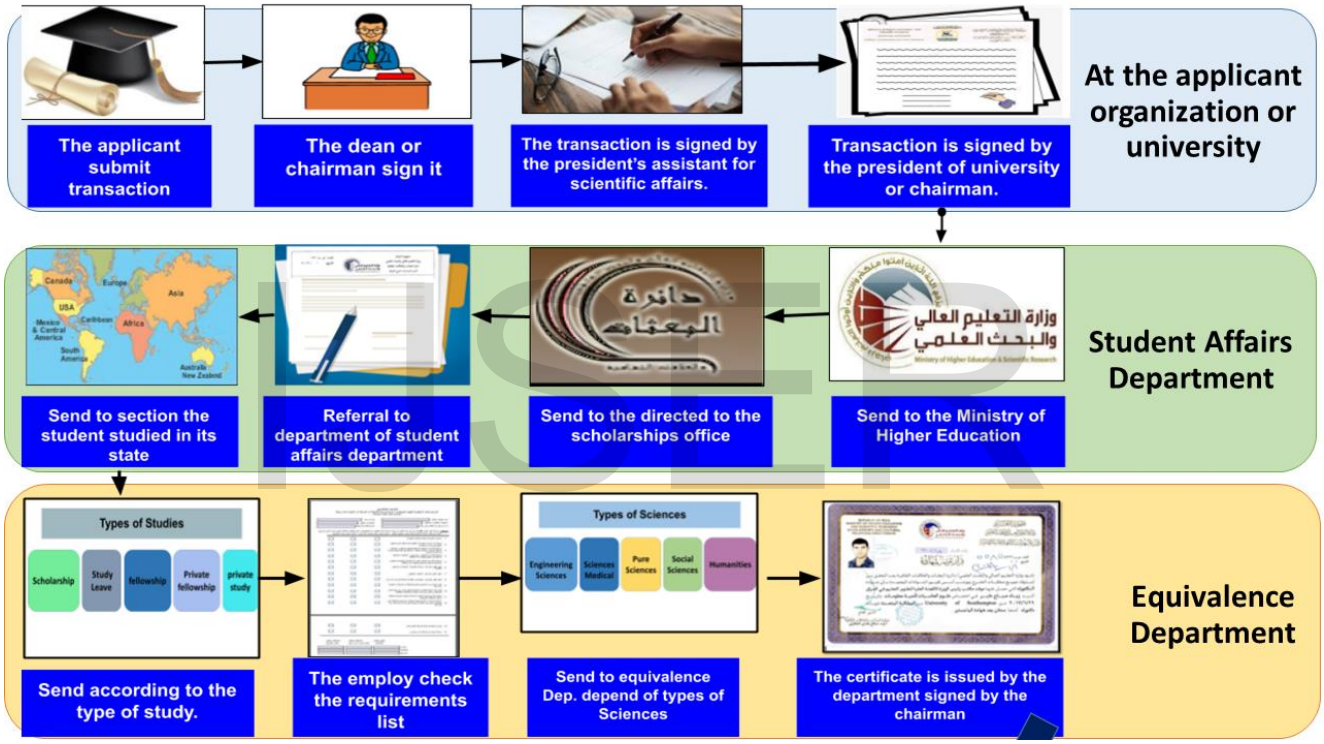


Figure 1. The Traditional Certificate Equivalence System

*B. When the certificate equivalence is completed, the following steps should be made for authentication:*

*I. At the applicant organization or university:*

1. The applicant resubmits the application with the certificate equivalence to the head of the department to add the certificate to his professional service history to get a salary increase.
2. The application is signed by the dean of the college or the chairman.
3. The application is signed by the president's assistant for scientific affairs.
4. The application is signed by the president of the university and referred to the Ministry of Higher Education (MOHESR) via confidential paper mail.

*II. At the Directorate of Scholarship and Cultural Relations (Equivalence Department):*

1. The application is referred to the Directorate of Scholarship and Cultural Relations in Iraq (SCRDIraq).
2. The application is directed to the equivalence department.
3. It is referred to one of the scientific sections which belong to his specific specialty.

4. The administrator refers it to the employee "n" to check the certificate equivalence in the Database, who's completed his certificate equivalence before.
5. After checking the authenticity of the certificate and if it exists in the Database, the employee writes a report then sends confident authentication for certificate equivalence. Otherwise, the fake certificate is terminated, as shown in figure 2. The section administrator signs the report after checking.
6. The report is signed by the head of the department after checking as well.
7. It is later signed by the chairman of the office or his assistant again after checking.
8. The transaction is copied and attested then sent via confidential paper mail to the Ministry of Higher Education (MOHESR), and resent to the university's applicant.

III. *At the applicant's organization or university:*

1. The university or organization will be approved the equivalence certificate incoming via confidential paper mail.
2. Issuance of an administrative order to the head of the department to add the certificate to the applicant's professional service history and increase his/her salary. The process is shown in Figure 2.

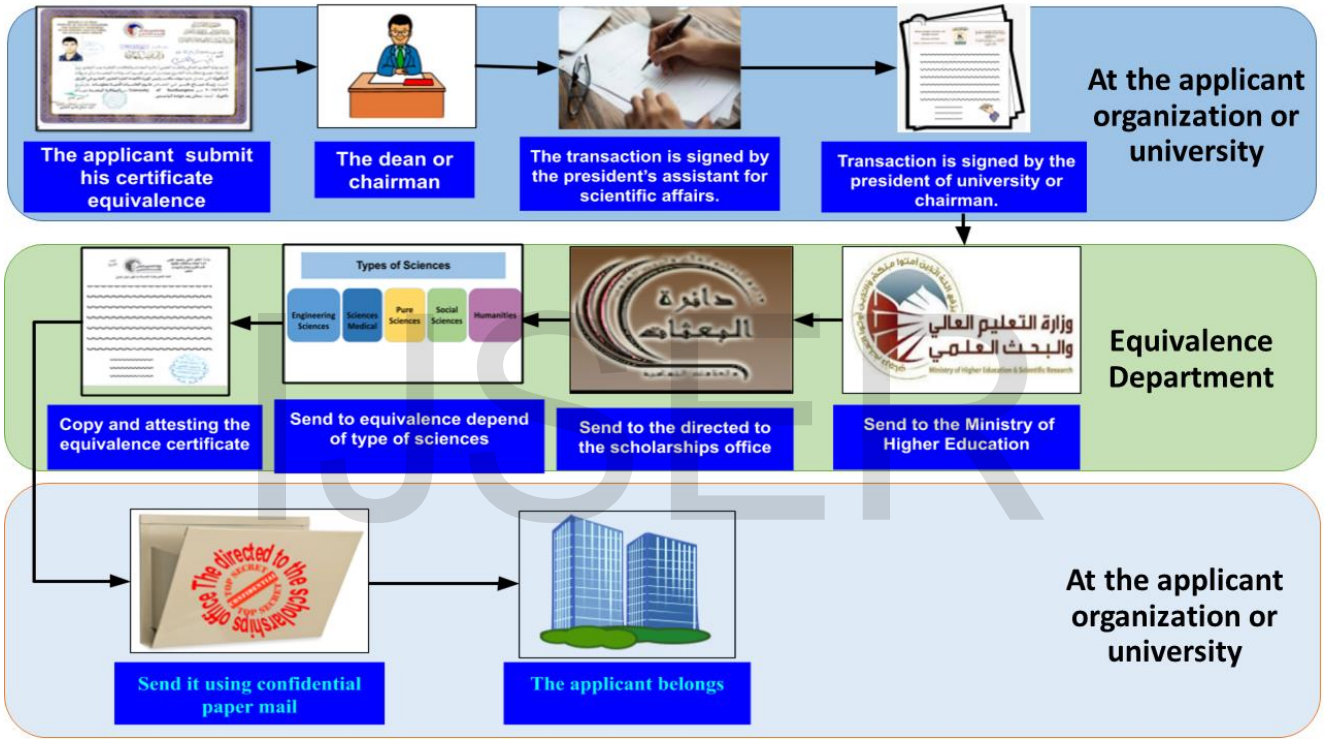


Figure 2. The Traditional Certificate Authentication System

## *III. THE CURRENT METHOD*

The current method differs from the traditional method by sending an additional copy of a completed equivalent certificate to the applicant's organization autonomously via confidential paper mail after attesting it and thus save effort, time, costs, and further transactions. An initial agreement has been approved by the Evaluation Department of the Directorate of Scholarship and Cultural Relations and submitted to the legal department. A special attesting procedure is expected to be implemented for validation.

The aim is to reduce the effort and time spent in the completion of the application and the data stored in the Equivalence office as this will eliminate the unnecessary duplication of documents.

Here we change the traditional certificate authentication system and use a new hyper model. Applying this procedure will lead to:

1- Eliminating steps (B. I to B. III), that is, 12 steps of administrative work.
2- Reducing the time of the transaction completion.
3- Reducing the effort of both parties: the applicant and the office in charge.

4- Reducing the costs of transportation.
5- Reducing copying papers (green solution).

A technique for issuing and revoking user certificates of authenticity in a public key cryptography system, wherein certificates do not need expiration dates, and the inconvenience and overhead associated with routine certificate renewals are minimized or avoided entirely. A Certification Authority issues certificates as required, and issues a blacklist having a start date, an expiration date, and an entry for every invalid certificate issued after the start date. Users assume that every certificate issued prior to the blacklist start date is invalid and that invalid certificates issued after the start date will be included in the current blacklist. A new blacklist is issued prior to the expiration of the current one, and the blacklist start date is changed only when the blacklist becomes unmanageably long, as shown in Figure 3.

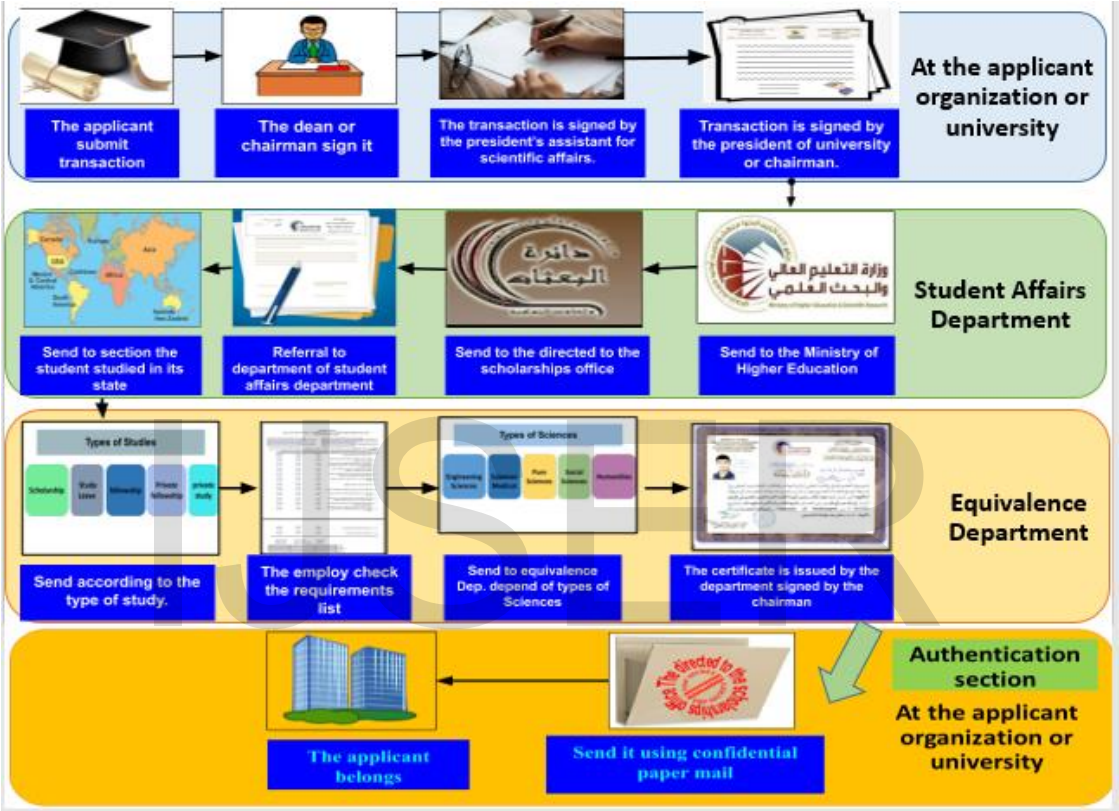


Figure 3. The Current Method of Certificate Equivalence Authentication

## *IV. THE PROPOSED METHOD:*

The proposed method differs from the traditional and current method by sending the web confident equivalent certificate as shown in Figure 4 to the applicant's organization autonomously via confidential paper mail after attesting it and thus save effort, time, costs, and further transactions. An initial agreement has been approved by the Evaluation Department of the Directorate of Scholarship and Cultural Relations and submitted to the legal department. A particular attesting procedure is expected to be implemented for validation.

The aim is to reduce the effort and time spent in the completion of the application and the data stored in the Equivalence office since this will eliminate the unnecessary duplication of documents.


| No. | Unified Iraqi National Card | Name | Belong to | Specialist | Foreign university | Iraqi university | Types of study | Transaction No. | Current status | Equalizer No. |
|---|---|---|---|---|---|---|---|---|---|---|
| 2912 | 198634128761 | Saleem Karim Mohamed | private | Atomic physics | Qatar University | University of Misan | private study | 5540/2018/03/08 | Complete | 31229 |
| 2913 | 197050258753 | Maher Hussein Kaoud | University of Dhi Qar | biological | Istanbul Technical University | University of Dhi Qar | private study | | In progress | |
| 2914 | 19690110796 | Maysa Selim Kamel | Ministry of Science | Fracture medicine | Tufts University | Baghdad University | Government Fellowship | 5557/2018/02/28 | Complete | 31247 |
| 2915 | 198970998787 | Zainab Saadoun Shaker | University of Diyala | civil engineering | TU Dresden | University of Salahaddin | Special Fellowship | | In progress | |
| 2916 | 199133180099 | Saadoun Shukr Khalaf | private | Anesthesia | Chiba University | University of Diyala | Study leave | | In progress | |
| 2917 | 199334190777 | Khairy Ragheb Karim | Rafidain University | Machinery Engineering | University of Savoy | Rafidain University | Government Fellowship | 5586/2018/03/30 | Complete | 31233 |
| 2918 | 198634128761 | Karima Ahmed Khair Allah | private | civil engineering | Sofia University | Baghdad University | private study | | In progress | |
| 2919 | 197038923466 | Salam Abdul Nabi Thujail | Al - Nahrain Iraqi University | Computer Engineering | University of Science, Malaysia(USM) | University of Babylon | Government Fellowship | | Lack of documentation | |
| 2920 | 198734327700 | Alireza Nasrawi | private | Genetic Engineering | University of Bucharest | Rafidain University | private study | 5500/2018/04/07 | Complete | 31240 |
| 2921 | 197834128875 | Sarah Karim Mahmoud | University of Al Mosul | Artificial intelligence | All India Institute of Medical Sciences | University of Al Mosul | Study leave | | Lack of documentation | |
| 2922 | 197497108780 | Ziad Sabah Aber | University of Karbala | Information Security | University of Southampton | Al - Nahrain Iraqi University | Government Fellowship | 5585/2018/02/18 | Complete | 31268 |

Figure 4. The Suggested Model of the web confident equivalent certificate

The suggested model still has the same steps of equivalence from 1 to 14 in addition to copying the certificate equivalences, attesting them by the office, and giving a number and date for equivalences. They are then uploaded to the web confident by the authorized employee using confidential mail.



### IV.1 Registration

For confident authentication, every ministry should have an administrator to do the registration and get a username and password to check the certificate equivalence and avoid the long routines. First of all, the authenticator signs up the verification by the official email of every ministry.

### IV.2 Getting the Certificate Equivalence Authentication.

After that, they sign in to the system if access is allowed to them. They will check the certificate equivalence number. If it is right, then the administrator can get their printed copies as a proof for Certificate Equivalence authentication. This is shown in Figure 5. Otherwise, he will wait till it is complete.


| No. | Iraqi National Identity | Name | Belong to | Specialist | Foreign University | Iraqi University | Types of study | Transaction No. | Current status | Equalizer No. | Equalizer Date |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 19657 | 199334190777 | Ziad Sabah Eabir | Bahgdad University | Information Security | University of Southampton | Bahgdad University | Government Fellowship | 5586/2018/03/30 | Complete | 31268 | 18/02/2018 |





Send via Web Confidential Mail

Figure 5. The printed copy as a proof for the Certificate Equivalence Authentication

The proposed method offers a solution to eliminate the unnecessary procedures, see section (B.I, B.II, and B.III). When the certificate equivalence is complete, the equivalent certificate is copied and attested by the office and given a number and date for equivalences inside the attestation. It will then be sent via confidential mail.

In this case, we will take a shortcut and stop the repeated steps in the transaction, reducing the steps of processing to complete the authentication.

A method to issue and revoke user authenticity certificates in a public key encryption scheme that requires no expiry date certificates and minimizes or avoids the inconvenience and overhead of regular certificate renewals. A Certificate Authority issues a blacklist that has a beginning, expiration, and entry for each invalid certificate issued after the start date, as needed. Users suppose that all certificates awarded before a blacklist start date are invalid, and the blacklist will include invalid certificates awarded after the start date. The new blacklist will be released before the present one expires, and only when the blacklist becomes uncontrollably long and the start date will be changed.

### IV.3 The Flowchart of the Existing System

In this part, the algorithm presents the interrelationships among four sides. The first side is the student/employee who belongs to a sponsor, like his university/ministry. He/She needs to get no objection to complete his study. The second side is the Iraqi academic student's data which provides his degree graduate. The third is the Iraqi Directorate of scholarship and cultural affairs which checks the compliance with regulations and laws of study board. The fourth side is the Foreign University and Student Office. This is shown in figure 6.

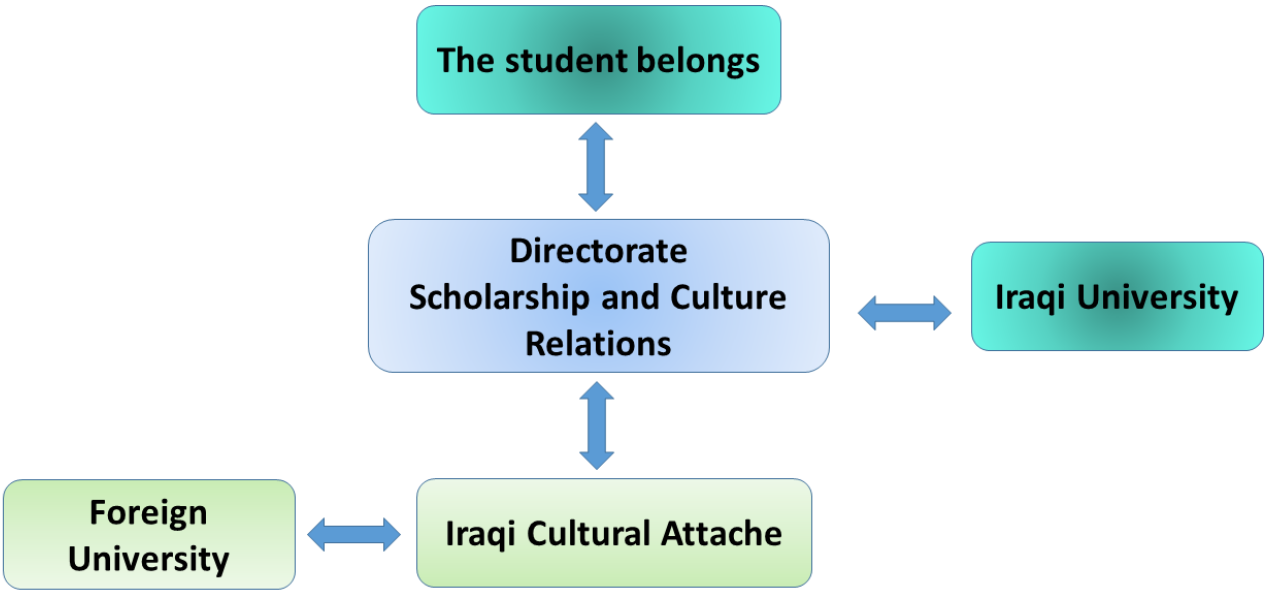


Figure 6. Check the flow chart of the certificate into and out of the country

IV.4 Algorithm of Suggested Authentication Model:

In this section, the authorized administrator must log to the Evaluation and Equivalence section. Based on the username and password entered, the administrator will check the certificate equivalence and complete his report as Successful Authentication or Unsuccessful Authentication as shown in figure 7.

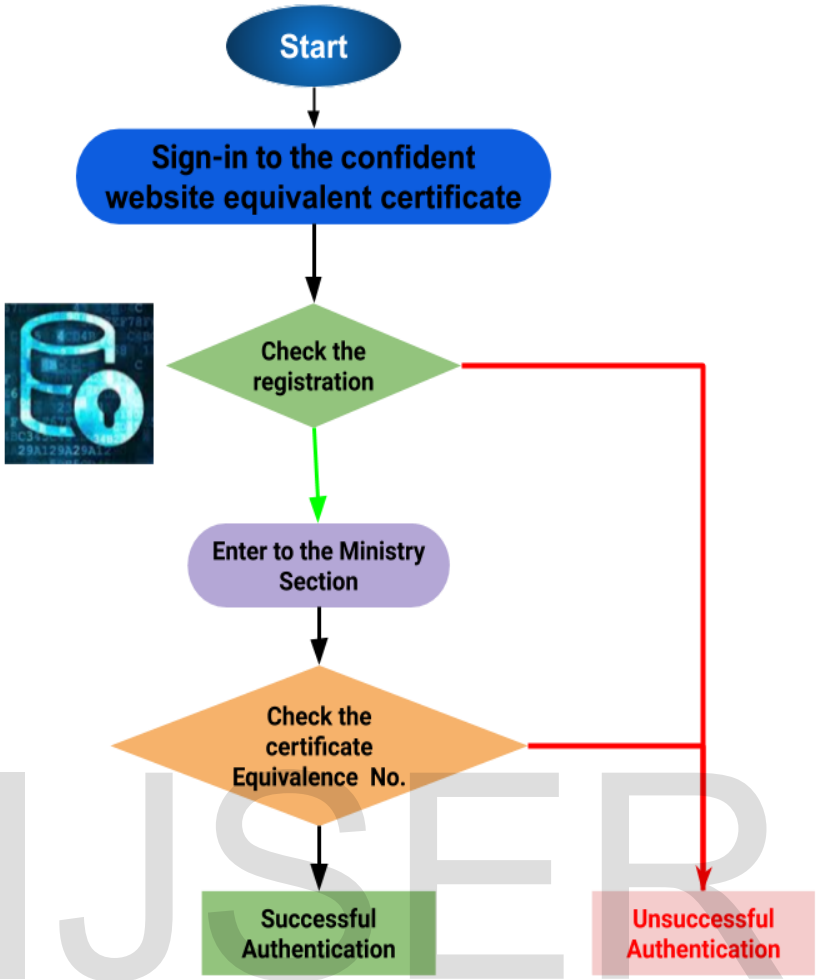


Figure 7. Algorithm of Authorization for Web-Based Information Systems

### IV.5 System Operations

If the government decides to use the web confidential and the INI as a unique number, this will make authentication faster and offer fewer steps, as shown in Figure 8:

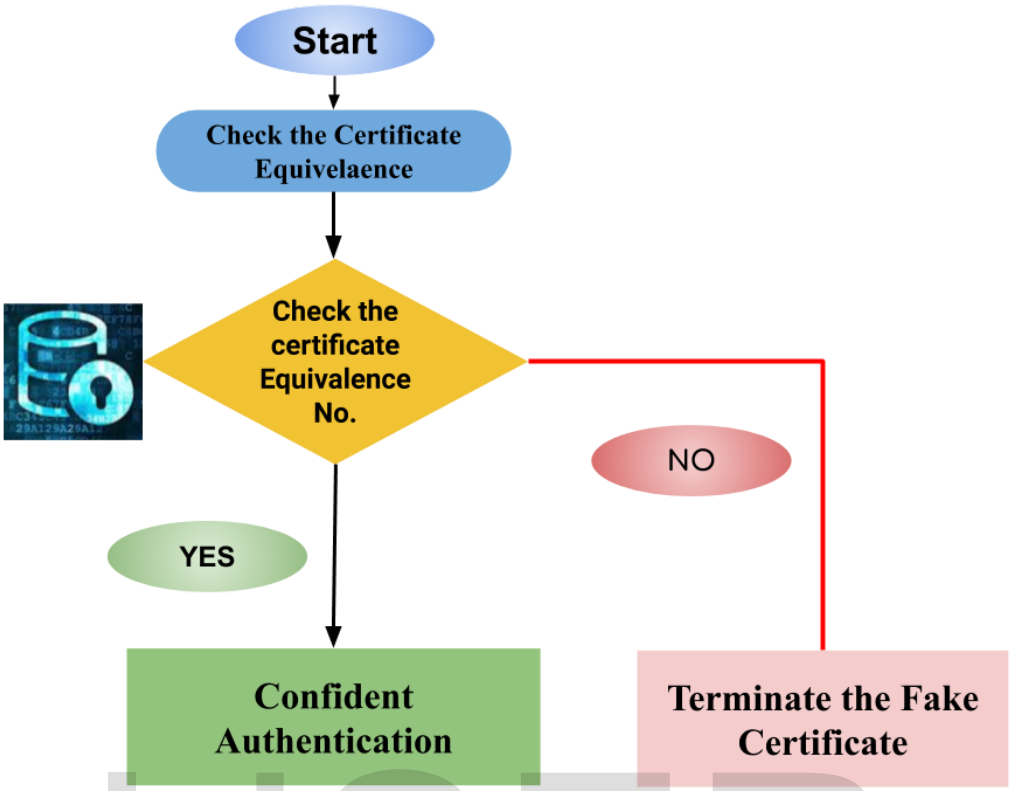


Figure 8. system operation for authorized access

The system gives each department username and a password. Authorized access by username and password is guaranteed in the Database. A special username and password are stored in the Database. Authorized users are encrypted. The system can show the status of the transaction and this helps the chairman and the employees to find the lack in the transaction.

### IV.6 Public Awareness

Issuance and authentication are still emerging disciplines. The level of the public awareness of these technologies and their usefulness is patchy and in many issues fraught with fault. This is prominently the case in homage to the protection and reliability of the technologies and their performance. It has been known that there is a little public awareness among government policy significance, business managers and individual users.

### IV.7 Performance Measures

Unlike the old issuance system, in the modern system, there is no need to print paper certificates or maintain old files. Instead, attestation is issued digitally, and auditable academic and professional credentials can be accepted anywhere, as shown in Table 1 below.

Table 1. The Benefits of Using New and Suggested Model

| Model | Time | Effort | Green solution | Authentication place |
|---|---|---|---|---|
| **Traditional** | 6 months or more | 32 steps of the equation | Double copying papers | At Equivalence Department |

| | | | | |
|---|---|---|---|---|
| **Current** | Less than 2 months | Less than 14 steps | Half copying papers | At Equivalence Department |
| **Suggested** | Less than a day | Three steps only | one copying paper | At workplace applicant |

### IV.8 Management Solutions

Here comes the question of why other ministries don't use the new administration like other countries. The Iraqi government creates the Iraqi National Identity (INI). In my opinion, not quite mature to deal with the democratic way should use compulsory ways with the path law to increases the ability to communicate, collaborate, and comply with the regulations. Building an assessment institute helps the government to monitor and control the effort of every employee. Increase public awareness it's not easy to accept the democratic way must use a compulsory way with the ability to choose the correct people in a proper situation, increasing training can help job satisfaction, employee motivation and reduce employee turnover.

The system gives every ministry a user name and a password, which the beneficiary needs for certificate equivalence and authentication. The authorized access of the data in the Database is guaranteed by means of checking the username and password. The authorized user's special username and password are stored encrypted in the Database.

### IV.9 System Operations

If the government decides to use the web confidential and the INI as a unique number, this will make authentication faster and offer fewer steps, as shown in Figure 9.



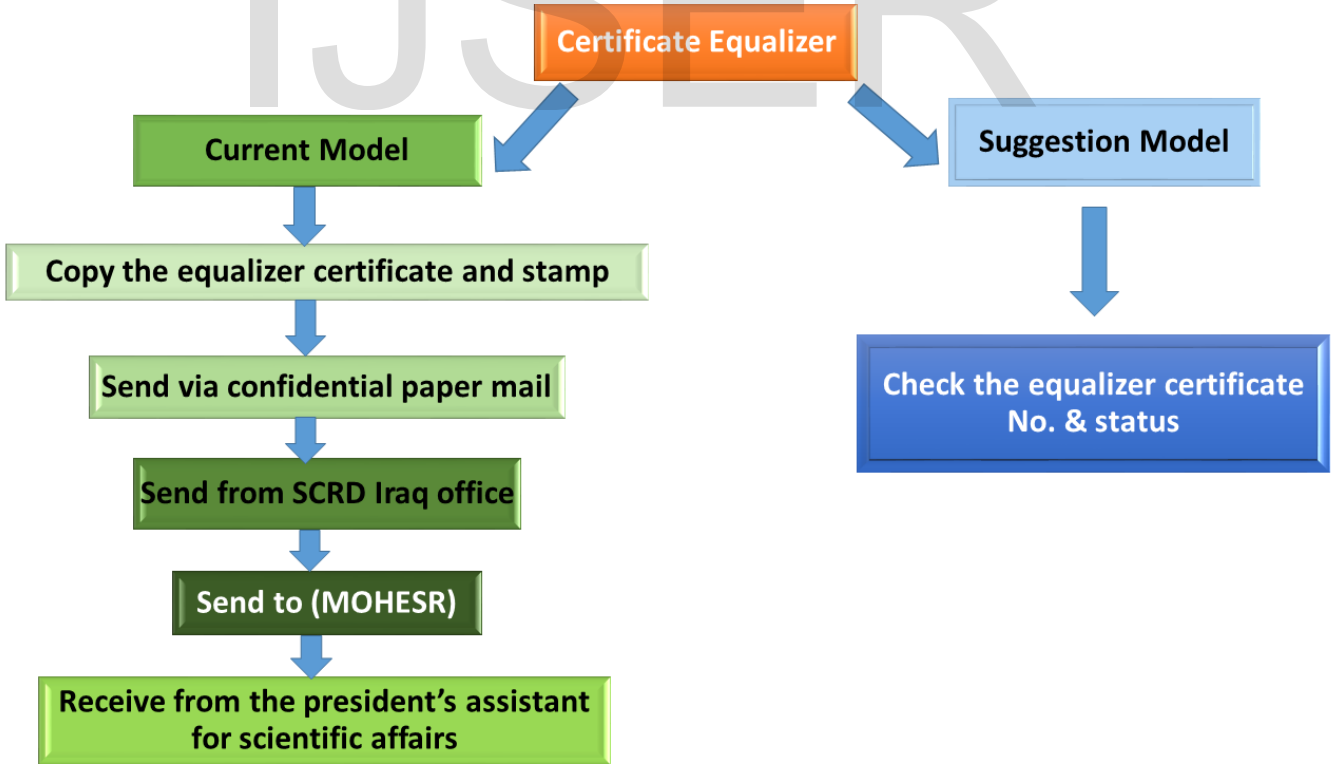


Figure 9. Current Model Compared to Suggested Model

### IV.10 Hardware and Software Issues.

The government didn't set up to provide the hardware part to let other ministries use INI. The other ministries, on their part, didn't try to involve the INI as a part of their official website either. In addition, the programs used are not licensed in most ministries.

## *V. Conclusion*

The new Iraqi government issued the Unified Iraqi National Card, so the question is why the other ministries don't use it. We recommend to the Iraqi government to use the suggestion model as an excellent solution. This technology can offer a way to address this problem by providing a secure solution without the need for confidential paper mail. By using the web confidential, we can make a shortcut for certificate issuance. It is easier to manage, giving it a better control of whose workplace applicants issuance certification and how they access it. The government worries about fake certificates, which may help forgers get a job in the government. So we suggest a hyper system to check certificate issuance. Using a web confidential authentication helps the citizen and lessens the cost and time spent. We also recommend using the website confidential and the Unified Iraqi National Card as a unique number. This will make it faster and reduces the effort exerted. Using digital certificates and digital signature improves the whole procedure. We advise the Iraqi government to use this model as a much better alternative.

In the future work, the proposed system is considered as a primarily steps toward establishing E-Government foundation related to the process of Certificate Authority to test the validity of certificate adhering the regulations of the Iraqi Directorate of Scholarship and Cultural Relation. The proposed system offers an improvement over the traditional paper-based system in term of the amount of time needed to carry out the validation procedure. We strongly recommend to apply the proposed system in the government organizations due to the significant enhancement in the certificate Authority procedure and in increasing trust between people the government organizations since it does not require the applicate to provide evident documents during various stages of the validation procedure.



## REFERENCES

[1]. Elwailly, F. F., Gentry, C., & Ramzan, Z. (2004, March). Quasimodo: Efficient certificate validation and revocation. In International Workshop on Public Key Cryptography (pp. 375-388). Springer, Berlin, Heidelberg.

[2]. Dodge, T., 2003, Inventing Iraq: The Failure of Nation-Building and a History Denied, London: Hurst

[3]. Dawisha, A. and Dawisha, K., 2003, How to Build a Democratic Iraq, in Foreign Affairs (May/June 2003). Lawson, C., 2003, How Best to Build Democracy: Laying a Foundation for the New Iraq, in Foreign Affairs, July/August 2003.

[4]. Dong, Z., Kane, K., & Camp, L. J. (2016). Detection of rogue certificates from trusted certificate authorities using deep neural networks. ACM Transactions on Privacy and Security (TOPS), 19(2), 5.

[5]. Kim, Yong Soon. "Challenges and Barriers in Implementing E-government: Investigation on NEIS of Korea." In 2006 8th International Conference Advanced Communication Technology, vol. 3, pp. 1635-1640. IEEE, 2006.

[6]. Durumeric, Zakir, James Kasten, Michael Bailey, and J. Alex Halderman. "Analysis of the HTTPS certificate ecosystem." In Proceedings of the 2013 conference on Internet measurement conference, pp. 291-304. ACM, 2013.

[7]. Mohammed MA, Kadhim MH, Fuad A, Jaber MM, editors. Follow up System for Directorate of Scholarship and Cultural Relations in Iraq. International Conference on Computer, Communications, and Control Technology (I4CT); 2014: IEEE.

[8]. Hyden, G., Court, J. and Mease, K., 2004, Making Sense of Governance: Empirical Evidence from Sixteen Transitional Societies, Boulder, Co:, Lynne Rienner.

[9]. Kimberly Stoltzfus, "Motivations for Implementing E-Government: An Investigation of the Global Phenomenon", Conference.04, Month 1.2 2004, City, State, - need to check ACM

[10]. Basu, S. E-Government and developing countries: an overview. International Review of Law Computers, 18, 1 (2004), 109-132.

[11]. Jaeger, P.T. and Thompson, K.M. E-government around the world: lessons, challenges, and future directions. Government Information Quarterly, 20 (2003), 389-394

[12]. Gupta, M. P. and Jana, D. E-government evaluation: a framework and case study. Government Information Quarterly, 20 (2003), 365-387.

[13]. Quasimodo: Efficient certificate validation and revocation. In International Workshop on Public Key Cryptography (pp. 375-388). Springer, Berlin, Heidelberg. using the Identify National Number can support the Simplification green solution.

[14]. Hayat, Amir, Reinhard Posch, and Herbert Leitold. "Identifying obstacles in moving towards an interoperable electronic identity management system." In eGOV INTEROP'05, 1st International Conference on Interoperability of eGovernment Services. 2005.

[15]. Durumeric, Zakir, James Kasten, Michael Bailey, and J. Alex Halderman. "Analysis of the HTTPS certificate ecosystem." In Proceedings of the 2013 conference on Internet measurement conference, pp. 291-304. ACM, 2013.