A SECURE E- MEDICAL EXEMPTION SYSTEM (E-MES): JORDAN CASE

Heba N. Kamel, Mohammad A. Alia, Bara'aha. Al Saeq, Eman Abu Maria

Faculty of Science and Information Technology – Al Zaytoonah University of Jordan, Amman, Jordan

ABSTRACT

In this paper, a new secure E- Medical Exemption System Based on Elliptic Curve Public Key Cryptography is proposed. This study specifies the medical exemption system in Jordan. However, the proposed system is summarized into three phases: first, the hospital process for applying the patient's application and producing the medical report. Second, the Royal Hashemite Court (RHC) process, which receives the hospital report, will then send a request to the ministry of health, the income and sales tax department, and the ministry of social development in order to check the patient's condition for a medical exemption. In fact, this aim of this step is to ensure that the patient is not able to bear the cost of treatment. Third, the RHC will send the decision to the patient via a short message. In practice, this E-medical system is more efficient than the traditional medical protocols since the patient can apply for a medical exemption directly from the hospital without suffering of any extra cost. Therefore, the elliptic curve public-key encryption and digital signature system ensures and guarantees the security of the proposed protocol. Nonetheless, to prevent a brute force attack, the choice of the key size becomes crucial.

KEYWORDS

Cryptography, Information security, medical system, and exemption.

1. INTRODUCTION

E-Government (Refer to Figure 1) is considered to be a way for governments to make them get able to make use of the most innovative information and communication technologies, particularly, web-based Internet applications, in order to provide citizens and different businesses [1]. There are other terms for defining the E-government. These terms comprise; Electronic Government, Electronic Governance, Digital Government, Online Government, E-Government, etc. The E-government resulting benefits can be less corrupted, increased in their transparencies, greater in their convenience, greater in their revenue growth, and/or in their cost reductions [2]. Further, there are four categories of E-government, which comprise; Government to Citizen (G2C), Government to Business (G2B), Government to Government (G2G) and Government to Employee (G2E). However, major government services depend on Government-to-Citizen (G2C) by providing citizens and others with different electronic resources in order to respond to the individuals' routine concerns and to the government transactions. Government and citizens can then communicate when implementing e-government, which will support accountability, democracy, and improvements to public services. G2B provides information for both governments and businesses. In addition, G2B includes various services like distribution of policies, memos, and rules and regulations.

DOI: 10.5121/ijnsa.2017.9202

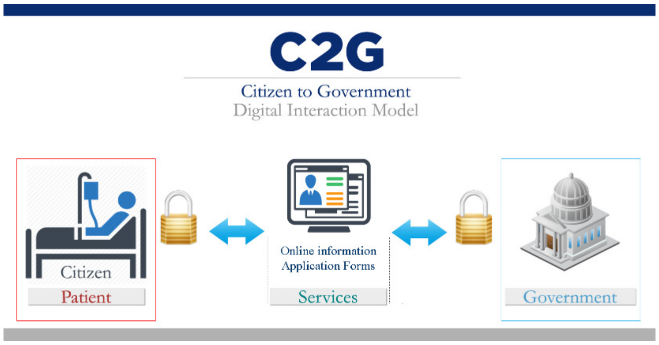

C2G
Citizen to Government
Digital Interaction Model
Citizen
Patient
Online information Application Forms
Services
Government

Figure 1: The C2G model

Such examples of the Business services include obtaining current business information, new regulations, downloading application forms, lodging taxes, renewing licenses, registering businesses, obtaining permits, etc. The G2G communicates between the government organizations, departments, and agencies by using online techniques through a super-government database. The main aim of the G2E is to assist the employees and to offer some online services, such as applying online for an annual leave, checking the balance of leave, and reviewing the salary payment records, among other things [2]. Most advantages of this category is to provide e-learning, which encourage knowledge sharing among them [2]. There are many services for E-government in Jordan, such as issuing certificates of non-criminal records, bookings of lending services, flyers and brochures, SDC website, investor identification and account set-up and transfers in cases of owning the shares of public shareholding companies, all can be found in the Hashemite Kingdom of Jordan [3].

A trust worthy medical system in some cases is crucial to a population's consent. The base of health is to help people freely. A significant motivating factor in the introduction of electronic exemption system is the elimination of medical forms. The technology of electronic medical exemption is used to provide support for the Jordanian patients in order to apply for a medical exemption. Besides, E-Exemption is a medical system that allows the patient to electronically apply his/her secure and confidential application. Meanwhile, E-Medical systems are generally using some advanced security tools. Therefore, elliptic curve cryptosystems are applied in this study.

2. Related Work

In Jordan, the e-government portal allows people to perform many services online in different departments, such as the Agricultural Credit Corporation, Amman Stock Exchange, Civil Service Bureau, Department of Land and Survey, Department of the National Library, Government Tenders Department, Housing and Urban Development Corporation, Income and Sales Tax Department, Insurance Regulatory Commission, Jordan Customs, Jordan Post, Legislation and Opinion Bureau, Ministry of Agriculture, Ministry of Finance, Ministry of Industry and Trade, Ministry of Interior, Ministry of Justice, Municipality of Greater Amman , National Information Technology Center, Royal Cultural Center, Royal Jordanian, Vocational Training Corporation, and the General Mufti Department [4].

2.1. E-Government and Medical Systems

The Abu Dhabi government provides full medical coverage for the entire UAE nationals living in Abu Dhabi. In cooperation with the National Health Insurance Company (Daman), the Abu Dhabi government introduces the new UAE national scheme, which is called the Thiqa.

Through thiqa, which is Arabic for "trust", Daman will provide the entire UAE nationals living in Abu Dhabi with a Thiqa card, which will replace their existing health cards. With the help of the Thiqa card, each UAE national will have comprehensive access to a large number of private and public health care providers who are registered within Daman's network. Further, it includes broader geographical coverage and extra health benefits.

In order to increase the accessibility, Daman provides a personalized "My Daman" page, which provides Daman card holders with the following features:

- Manage Your Claims: submit and track claims.
- Online Endorsements: add, edit, or cancel members.
- Member Guide: browse through a health insurance knowledge database.
- Request Call Back: submit a request to have one of Daman's agents call you back.
- Feedback: provide your feedback regarding Daman's services [5].

2.2. The Traditional Medical Exemption System (MES)

In 2012, his Majesty King Abdullah II shared the opening of the public service office for the people who do not own any insurance health, or who cannot afford paying the cost of their health treatment, which is very expensive for them to carry on. His Majesty gave his order in order to open an office in Raghadan Palace. The patient must bring the following documents by himself or some of his first degree relatives to this office [6]:

1. Valid personal identification.
2. Valid family book.
3. A medical report non-judicial for the patient.
4. The patient must be resident in Jordan.
5. The patient has no medical insurance.

After the patient delivers the papers to the office, the employee then waits for a while until the requirements held by the ministries and departments are checked. After that, the patient is given the medical treatment exemption along with the name of the hospital that will take part in treating this patient who is said to apply for the medical treatment exemption.

2.3. Information Security and Cryptography

Information security is the process that describes the entire measures, which are taken to prevent any unauthorized use of the electronic data in terms of whether this unauthorized use takes the form of destruction, use, disclosure, modification, or disruption. The information security and cryptography are interconnected and can share the common services of protecting confidentiality, integrity, and the availability of the information that is ignoring the data form (electronic document, printed document). In the encryption process, the information security uses Cryptograph in order to shift the information into a cipher form, which does not allow it to be used by an unauthorized person [7].

Cryptography is one of the most important fields in computer security. In fact, it is a method of transferring private information and data through an open network communication, so that only the receiver who has the secret key can read the encrypted messages, which might be documents, phone conversations, images, or other forms of data [7].

Furthermore, Cryptography contributes to computer science, particularly, in the techniques that are being used in computer and network security for control access and information confidentiality. Cryptography is also used in many applications encountered in our everyday life, as such computer passwords, ATM cards, and electronic commerce.

ECC CRYPTOGRAPHY

Nowadays, Elliptic Curve Cryptography (ECC) acquires a lot of attention due to its small key size for encryption, decryption, and digital signature processes, where these made it to be widely being used between the durations of 2004 and 2005. ECC was discovered by Koblitz [8], and Miller [9]. The ECC schemes are public-key mechanisms that provide the same functionality as RSA schemes provide. Nonetheless, their security is based on the hardness of a different problem, namely the Elliptic Curve Discrete Logarithmic Problem (ECDLP) [10]. The adoption for ECC makes it competitive to RSA, since it can reach the same security level with smaller key size. In fact, smaller key size means less computation time and high performance speed. The ECC can be used in various areas, such as in encryption algorithms like ECIES, which is replaceable for RSA cryptosystem, or key exchange protocol, such as ECDH, or as a digital signature, such as ECDSA, which is recently being intensively used through the Internet in order to provide integrity and non-repudiation for messages. Elliptic curve protocols depend on the ECDLP, which assumes that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is considered infeasible [11].

ECIES AND ECDSA PROTOCOLS

The ECIES and ECDSA algorithms [12] are defined on the same selected prime curve. The ECIES generates its public and private keys, and the ECDSA performs the same by generating the public and private keys. Figure 2 shows the combination results of the ECIES and ECDSA protocols. The proposed protocol comprises the following main steps:

1. Encryption
2. Signature
3. Verify signature
4. Decryption

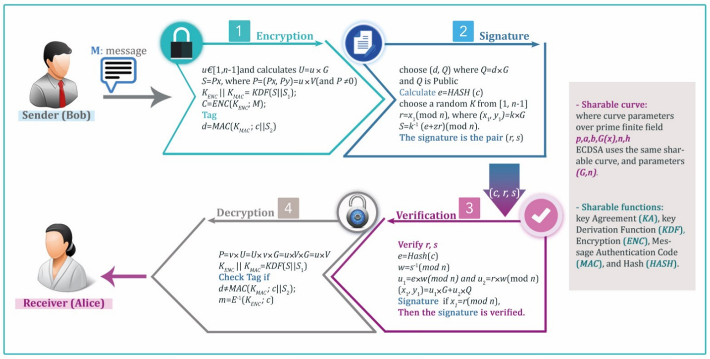

M: message
Sender (Bob)
1 Encryption
u€[1,n-1]and calculates U=u × G
S=Px, where P=(Px, Py)=u×V(and P ≠0)
K_ENC || K_MAC = KDF(S||S_1);
C=ENC(K_ENC; M);
Tag
d=MAC(K_MAC; c||S_2)
2 Signature
choose (d, Q) where Q=d×G
and Q is Public
Calculate e=HASH (c)
choose a random K from [1, n-1]
r=x_1(mod n), where (x_1, y_1)=k×G
S=k^-1 (e+zr)(mod n).
The signature is the pair (r, s)
(c, r, s)
3 Verification
Verify r, s
e=Hash(c)
w=s^-1(mod n)
u_1=e×w(mod n) and u_2=r×w(mod n)
(x_1, y_1)=u_1×G+u_2×Q
Signature if x_1=r(mod n),
Then the signature is verified.
Decryption 4
P=v×U=U×v×G=u×V×G=u×V
K_ENC || K_MAC=KDF(S||S_1)
Check Tag if
d≠MAC(K_MAC; c||S_2);
m=E^-1(K_ENC; c)
Receiver (Alice)
- Sharable curve:
where curve parameters over prime finite field
p,a,b,G(x),n,h
ECDSA uses the same sharable curve, and parameters (G,n).
- Sharable functions:
key Agreement (KA), key Derivation Function (KDF), Encryption (ENC), Message Authentication Code (MAC), and Hash (HASH).

Figure2: The proposed ECIES and ECDSA protocols

The advantages of the combination between the ECIES and ECDSA protocols:

1. They are easy to be implemented for certificates by using the ECDSA protocol, which will increase the authentication level.
2. Both algorithms depend on the ECC. Thus, they use the same curve parameters, which add more flexibility for implementation.
3. Adding another authentication, namely ECDSA signature, for a chosen text along with the ECIES authenticator, which depends on the HMAC.

3. The Proposed Electronic Medical Exemption System

In general, the proposed method describes the whole procedures that help the patient to have medical exemptions from the hospital without the need to worry about any matter. Meanwhile, the proposed system is based on the Elliptic curve cryptosystem (Encryption/Digital signature) in order to enhance the security purposes, since this system is accessed over the open network. The proposed system aims at assisting patients that have different healthy cases to prepare the required documents in order to apply for the medical exemption, since this process is successfully performed via the electronic system without any further assistance.

As shown in Figure 3, the patient must visit the hospital in order to apply for the RHC exemption report. In this process, the patient must provide his/her authentication by using the National ID in order to assure that this system is just valid for Jordanian patients. However, a medical test is issued to complete the exemption process. In Figure 3, Step 2 shows that the RHC receives the secured medical report from the hospital, since this report is encrypted by the RHC public key, and is signed by the hospital private key based Elliptic curve cryptosystem. On the other hand, the secured report is decrypted and is verified by the RHC, as shown in Figure3, particularly, in Step 3. Besides, the RHC distributes the patient request to the Ministry of Health, the Income and Sales tax department, and the Ministry of Social development securely by using the Elliptic curve cryptosystem. In particular, these departments send a secured feedback to the RHC, which describes the applicable situation. Furthermore, the RHC evaluates the patient case to give the final decision (Refer to Figure 3, Steps 3 and 4). As mentioned previously, the final decision is sent securely to the concerned hospital. In addition, this decision is sent to the patient. Nonetheless, the decision might be accepted or rejected according to patient's case record, and to the RHC procedure. Further, the patient should follow the previous steps in order to renew his/her medical exemption.

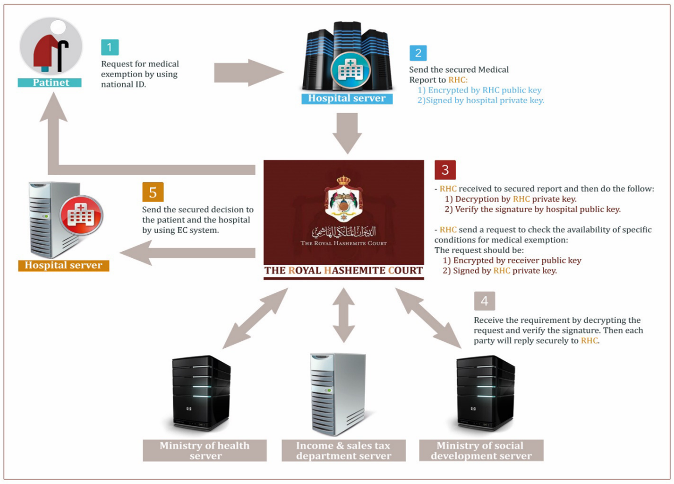

Patinet
1
Request for medical exemption by using national ID.
Hospital server
2
Send the secured Medical Report to RHC:
1) Encrypted by RHC public key
2)Signed by hospital private key.
3
- RHC received to secured report and then do the follow:
1) Decryption by RHC private key.
2) Verify the signature by hospital public key.
- RHC send a request to check the availability of specific conditions for medical exemption:
The request should be:
1) Encrypted by receiver public key
2) Signed by RHC private key.
الديوان الملكي الهاشمي
The Royal Hashemite Court
THE ROYAL HASHEMITE COURT
5
Send the secured decision to the patient and the hospital by using EC system.
Hospital server
4
Receive the requirement by decrypting the request and verify the signature. Then each party will reply securely to RHC.
Ministry of health server
Income & sales tax department server
Ministry of social development server

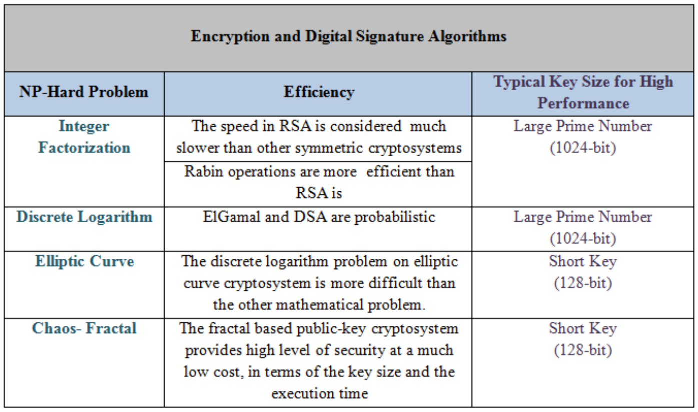
Figure3: The proposed E-MES based EC system

The benefits of producing the MES system is to save time for doctors, other medical staff, and employees in the RHS. For instance, there is no need to have a place for people to wait longer than normally should be, or there is no need for other medical staff or other employees to take the papers to read them in order to check as to whether these papers are valid or not. In practice, everything is being conducted via computers where there is no need for more papers or extra employees.

In addition, some people complain that they must leave their works for several days in order to perform the procedure of exemptions for their relatives where there is no need any more to obtain the medical exemption report personally but can be obtained anywhere online.

4. Performance Evaluation based on Equivalent Key Sizes for Elliptic Curve and Public-Key Cryptography Protocols

The Authors compare the performance of the combined Elliptic Curve based public-key algorithm against the well-known primes based public key algorithms (for example, RSA and DSA) [13]. Nevertheless, the examinations shows that integers based public-key algorithm (ECC) provides higher level of security at a much lower cost, both in term of key size and execution time. Besides, Table 1 demonstrates the key size for prime based algorithms (RSA, DSA, etc.) and integer based algorithm (ECC, Chaotic), with respect to the imperviousness to brute force attacks. However, the keys space for RSA and DSA were calculated based on the number of primes existed for particular key sizes [14].



Encryption and Digital Signature Algorithms		
NP-Hard Problem	**Efficiency**	**Typical Key Size for High Performance**
Integer Factorization	The speed in RSA is considered much slower than other symmetric cryptosystems	Large Prime Number (1024-bit)
	Rabin operations are more efficient than RSA is	
Discrete Logarithm	ElGamal and DSA are probabilistic	Large Prime Number (1024-bit)
Elliptic Curve	The discrete logarithm problem on elliptic curve cryptosystem is more difficult than the other mathematical problem.	Short Key (128-bit)
Chaos- Fractal	The fractal based public-key cryptosystem provides high level of security at a much low cost, in terms of the key size and the execution time	Short Key (128-bit)

5. Conclusion

This paper shows the possibility of establishing an E-exemption medical system based on a public-key encryption cryptosystem. The security of the proposed E-Exemption depends on the elliptic curve public key encryption and on the digital signature protocol. The proposed protocol is more efficient than other E-medical systems in Jordan. It allows patients who do not have medical insurances in Jordan to obtain the exemption directly from the hospital system at no extra cost and effort. With the emergence of the new technology that is based on the electronic e-xemption system, the proposition of this system aims at replacing the previous conventional medical exemption system, since patients feel confident that their applied medical exemption is being counted and processed truly. Moreover, the proposed system only needs the basic requirements, such as the standard mobile phone, and the website, in order to obtain the exemption report acceptance.

Acknowledgment

The authors would like to thank Al-Zaytoonah University of Jordan for their efforts in supporting this study.

REFERENCES

[1] Mohammed Alshehri and Steve Drew School of ICT, Griffith University Brisbane, Australia“E-GOVERNMENT FUNDAMENTALS, ” IADIS International Conference ICT, Society and Human Beings 2010.

[2] Hiba Mohammad, Tamara Almarabeh and Amer Abu Ali, “E-government in Jordan,”European Journal of Scientific Research. ISSN 1450-216X Vol.35 No.2 (2009), pp.188-197.

[3] The Official Site of the Jordanian e-Government. Available from World Wide Web: http://www.jordan.gov.jo/wps/portal/!ut/p/c5/04

[4] The Official Site of the Jordanian e-Government .Available from World Wide Web: http://www.jordan.gov.jo/wps/portal/!ut/p/b1/jc_PDoIwDAbwZ

[5] The Abu Dhabi eGovernment Gateway. Available from World Wide Web: https://www.abudhabi.ae/portal/public/en/citizens/health/health_insurance/gen_info44?docName

[6] KING OF THE HASHEMITE KINGDOM OF JORDAN.Available from World Wide Web: http://www.kingabdullah.jo/index.php/ar_JO/news/view/id/9817/videoDisplay/1.html

[7] Menezes, A., P. Van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography," CRC Press, pp.4-15, 516, 1996.

[8] N. Koblitz, “Elliptic Curve Cryptosystems,”Mathematics of Computation, vol. 48, no. 177, p. 203–209, 1987.

[9] V. Miller , “Use of elliptic curves in Cryptography,” Springer-Verlag, vol. CRYPT0 '85, no. LNCS 218, pp. 417-426, 1986.

[10] D. S. Kumar, C. Suneetha and A. ChandrasekhAR , “Encryption of data using elliptic curve over finite fields,” International Journal of Distributed and Parallel systems, vol. 3, no. 1, pp. 301-308, 2012.

[11] V. G. Martinez, L. H. Encinas and C. San, “A survey of the elliptic curve integrated encryption scheme,” Journal of Computing Science and Engineering, vol. 2, no. 2, pp. 7-13, 2010.

[12] Ehab M. Alkhateeb, M. A. Alia, and A. A. Hnaif. “The Generalised Secured Mobile Payment System Based on ECIES and ECDSA”. ICIT 2015 The 7th International Conference on Information Technology doi:10.15849/icit.2015.0055 © ICIT, Jordan, 2015.

[13] M. A. Alia. “Combining Public-Key Encryption with Digital Signature Cryptosystems”. Proceedings of the International Conference on Advanced Intelligent Systems and Informatics. Springer, 2016.

[14] B. Elaine, W. Barker, W. Burr, W. Polk, and M. Smid, “Recommendation for Key Management – Part 1: General,”NIST Special Publication 800-57, 2006.