A Mechanism using the Electronic Signature to Verify the Power of Attorney and the Requested Activity

Wadee Alhalabi
Department of Computer Science
Faculty of Computing and Information Technology
King Abdulaziz University
wsalhalabi@kau.edu.sa

Reem Ahmed A. Almasoudi
The 35th Intermediate School
Ministry of Education
reem-22@hotmail.com

Abstract--- The rapid development that accompanies computer and information technology imposes its applications on all societies in general and developed countries in particular. In this paper, we present an algorithm to apply the electronic signature to verify the credibility of power of attorney and the credibility of activity requested using power of attorney. The verification algorithm is to be used in courts of law; the algorithm ensures a credible approval by the owner to the agent who has the power of attorney to submit the activity under concern. Selling a real estate property is an example of an activity which might be conducted by the agent using the "power of attorney".

This system, which we designed, implemented and tested, takes into consideration all the financial and security information needed. Our system requirements adopted the financial requirements such as banks and financial firms in number of societies and countries such as the United States, the European Union and Jordan.

Keywords: Smart Trash Bin, Local Base Station Smart Vehicle System, Smart Monitoring and controlling Hut, Control Panel, Data Control, Unique Trash Bin Code.

*****

I. INTRODUCTION

Technical development has become influential in many areas in our daily life, this includes the justice system. The matter of utilizing the algorithm is well-known even in countries like Saudi Arabia. It is usually known that people go to courts to issue a "power of an attorney". Most of the time, this person is a family member such as a brother, a husband or a son. We will call this person "the representative". The representative can attend on behalf of the owner this even includes the meetings in which the owner has to be present in person. The main problem is the abuse of the power of attorney by "the representative". This algorithm is going to prevent this abuse. An example of an abuse is, the representative goes to court to sell a property without the owner awareness.

Electronic signature was already used in court in a number of developed countries such as the United States of America, the European Union countries and Japan. In order to be judicially adopted, that necessitated security to be there to ensure information on the international standard X-800, which provide the information security with the following:

1. Verification of the system user (Authentication).
2. Prevent unauthorized persons from accessing the system (Access Control).
3. Data encryption to ensure confidentiality (Data confidentiality).
4. Information integrity to ensure that the data has not been altered (Data Integrity).
5. Providing information with the means to ensure information cannot be sent by other than the sender (Non-Repudiation).

II. PREVIOUS STUDIES

Ed McNachtan et. al. presented a study [1] showing 19 courts in the State of Ohio adopted the electronic signature in 2006. As a worksheet might be proposed in the Ohio justice conference calling for the application of electronic signature in all branches of the courts in the state, and the state of Washington is also considered the largest state in the U.S. supporting electronic treats in courts.

In a detailed study Reda [2] showed that countries such as France, Belgium, Austria, China, Malaysia has legislated laws and legislation governing electronic signature in particular, and digital trading generally. These countries also developed laws and regulations that ensure the correct use and studied the legal effect and protecting the legitimate rights and interests of all

parties as EU law confirmed the legitimacy of electronic signatures. There are also laws issued by the Department of Justice, Department of Communications and the Department of International Trade and Industry in The States. As an example is the Supreme Court Act of Ohio (digital signature is widely defined as follows: electronic signature is an electronic sound, symbol, or process logically associated with a record and executed by the person who signs this record). The current rules allow the court to record documents in court electronically. There are also some of the Arab countries endorsed the use of electronic signature, including Jordan, Egypt and Tunisia, in addition to Dubai special law of transactions and electronic commerce.

III. ELECTRONIC SIGNATURE

3.1 The definition of an electronic signature

Electronic signature is an encrypted mechanism to authenticate transactions online. The idea of the electronic signatures is to do the same as the handwritten signature. It is used for ratification and is associated to the site identity for a transaction.

3.2 The mechanism of the electronic signature

Electronic signature involves two processes; the first one is completed by the site and the other one is by the recipient as shown in Figure 1.

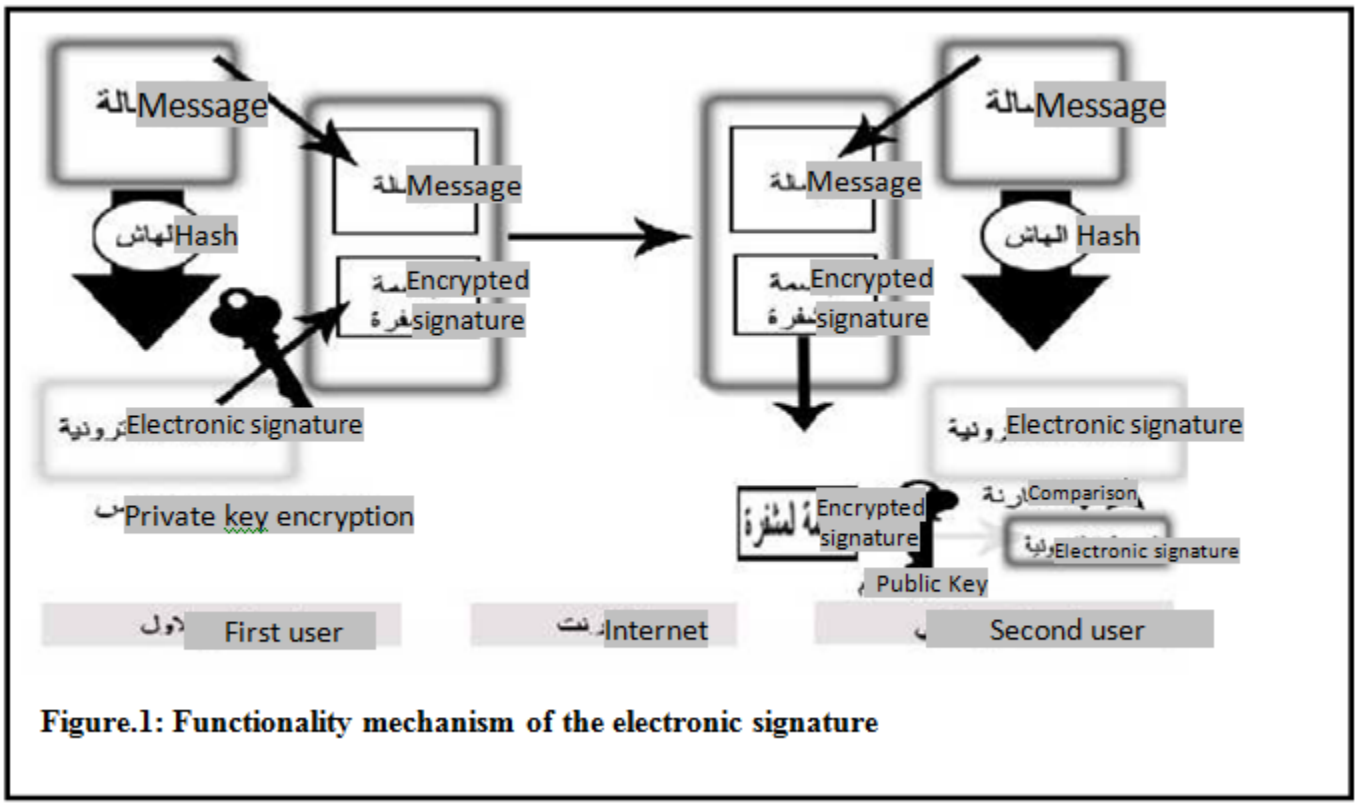

Figure.1: Functionality mechanism of the electronic signature

3.3 Creating an electronic signature

The output of the hash code is used to create the electronic signature. The hash is a one-way mathematical function. An example of a hash function is a function is the rounding function, or the mod function.

If we use the mod function for instance to find the value of 17 mod 5 = 2

This function is irreversible and if 5 and is given, we cannot determine the value of 17 as there are infinite number of values X where X mod 5 = 2.

Using the hash in a message:

We give each characters a weight A = 1, B = 2, ... Z = 26. We can turn every character in to a number.

If we assume that the summation result of a message letters was 132135197; still fit on the hash function we choose mod 71419, the result is 10047.

This is a special sign of the message. Then we can use any method of encryption and signing using either the private or the public key or symmetric keys used in the information security.

3.4 Sign the massage using private key and open the massage using the public key

A private key is given to each person and is used to sign his message. The public key is given to the other party to open the message and verifying the signature.

For example:

$$C = M^e \bmod n , \quad M = C^d \bmod n$$

Where e is a special number to encrypts the message M to produce a code or a signature C

This signature is true if we use d to verify the signature

If we used key (d_1) for the code (C), the output would be true if appeared to us the message (M).

There is no key other than (d_1) that could open the code of the signature (e_1).

This is the most common way in using electronic signature, so the key(e_1) has only one key to open the massage key (d_1).

The key(e_2) has a key (d_2), and the key (e_n) has a key (d_n).

IV. ELECTRONIC AUTHORIZATION

4.1. The definition of electronic authorization

It is a method by which, verification of the contracts concluded by the legal agent who has the power of Figure 2 explains this scenario.

4.2. Motivations:

Require the approval of the owner in a safe and accessible on text via the Internet to ratify the contracts and record in the courts. This limits crimes, the unethical acts and manipulation and exploitation of legitimacy authorizations that were occurring previously in the absence of the client thus providing full protection for client under the age of safe information system.

4.3. Functionality mechanism of the electronic authorization

Implementation steps (sales contracts as an example):

1. The agent signs the contract in question.
2. The agent send contract approval request to the owner then waits for the electronic signature by the owner for the approval of the contract ratification in the court.
3. The owner reviews the contracts and then approves it using his electronic signature and sends the contract back to the court directly.
4. The court receives the owner's approval after the verification of the signature and then makes ratification of the contract and complete sale procedures.

Figure.2: Functionality mechanism of the electronic authorization

V. SUMMARY

This algorithm which we have introduced here will stop a large number of financial crimes which are committed by the agent who has the power of attorney. We also found that the electronic system provides a safe cover benefiting the client in keeping his rights.

For example people with special needs who cannot attend court or women who find it difficult to move, all those and others will get the advantages of this system which provides them with a mechanism that is equivalent to the attendance for the courtroom to complete their judicial procedures such as sales safely.
We recommend an immediate implementation of this algorithms in courts.

VI. REFERENCES

[1] Ed McNachtan, Jim Mendel, Mary Beth Parisi, Chere 'Evans. Technology and the courts. The Supreme Court of Ohio.

[2] Authentic electronic signature legal adviser ,Dr. Ali Reda.

[3] Thomas Zachman ,Guy C.Guckenberger .Electronic Signatures Report, Ohio Judicial Conference, November 2004

[4] http://www.ohiojudgcs.org/_cins/tools/act_Download.cfm?FiIeID=482&/Report%2OElcc%2OSigs.pdf

[5] Brief about Electronic Signatures. Ministry of Communication and Information Technology of the Arab Republic of Egypt.

[6] http://www.e-signature.gov.eg/materials/ElectronicSignature_Mechanizm_Arabic.doc