Scientific Research Publishing

Beijing Law Review, 2016, 7, 357-370
http://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Use of E-Signature in Proof of Contracts Concluded through the Internet in Jordan

Ahmed Al-Nuemat[1], Mohammad AL-Thunibat[2]

[1]Al-Balqa Applied University, Amman, Jordan
[2]Middle East University, Amman, Jordan
Email: ahmed_alnuemat@yahoo.com

How to cite this paper: Al-Nuemat, A., & AL-Thunibat, M. (2016). Use of E-Signature in Proof of Contracts Concluded through the Internet in Jordan. *Beijing Law Review, 7,* 357-370.
http://dx.doi.org/10.4236/blr.2016.74030

Received: September 6, 2016
Accepted: December 25, 2016
Published: December 28, 2016

Abstract

The last few years, more specifically since 1995, have seen very important developments in the networking and technology of electronic commerce. The e-signature is one of these technologies working toward electronic commerce. A major issue highlighted and appropriately discussed in this article is regarding the parameters identifying an e-signature and authenticating the same. The current form of the Electronic Transaction Law (ETL) provides for two different ways for verifying e-signatures, which at times creates ambiguity. With regard to the major defect that the provisions and rules of the ETL create, in respect of the validity of an e-signature and an authentic signature in proof, the authors see that the ETL should clearly provide that an e-signature shall have a validity in proof the same as the traditional signature, while an authentic e-signature shall have a validity in proof the same as a written signature.

Keywords

E-Signature, E-Contracts, Internet, Jordan

1. Introduction

The electronic signature is described in Article (2) of the Electronic Transaction Law (ETL)[1] as:

"*Electronic, numeric or photo data or others taking the shape of letters, numbers, symbols, or signs, or the like in a data message or added or related thereto, having a shape identifying the person who timed or distinguished it from others for reasons of the person's signature and the approval of content*".

The law takes into account the purpose of the electronic signature and considers it to be the same as the conventional signatures used. For example, the conventional signa-

[1]Electronic Transaction Law No. (85) of 2001.

ture can be used as evidence, as a ceremonial function, as a designation of approval, and as a determination of authenticity. An electronic signature can fulfil all of these purposes without changing the existing paradigm of a person "signing" a document. So the electronic signature has all the functions to be equivalent to the conventional signature.

It can clearly be seen that the definition of the electronic signature is not well thought of and it does not explain the issuance of the signature and the process for the authentication of the signature. However, the legislation codified the validity of an e-signature and its functions in Article (10/b), as it states:

"*b-The validity of the signature shall be proven and attributed to the person signing the electronic record when there is a method to identify that person and to indicate his approval of the information contained in the electronic record that carries his signature, if that method is reliable for this purpose in light of the circumstances relating to the transaction, including the parties' agreement to using this method*".

Accordingly, the functions of the e-signature are:

- Identification of the person related to the electronic signature. The contracting parties can also use the other options which the internet makes available. These options include the Digital ID or the personal certificate. This can be done to verify the identities of the people participating in the contracting process.
- The electronic signatures also show the consent of the person concluding the contract. It shows that the person who has used the electronic signature agrees to the legal framework of the contract and to fulfil the obligations that are set out in the contract.

Besides these two major functions, the e-signatures also follow the conditions provided by the Jordanian legislature. These conditions are the objective conditions and the formal conditions.

2. Objectivity Conditions

The clauses of the ETL state that the Jordanian laws require the following conditions: the verification of the e-signature and the conditions of the e-signature. The conditions mentioned are described below:

2.1. Authentication

The verification of the e-signatures is taken as the major condition which needs to be fulfilled as required by the Jordanian laws. It is stated by Article (30) of the ETL that the e-signatures are taken as evidence for the legality of the consent of the contracting party. The verification procedure is specified in Article (30/a). The details of the process can be found in the clauses of the ETL. These are stated as follows:

1) The verification process should be an approved process. The approval is done by issuing the necessary process from a governmental or non-governmental agency with the responsibility of verifying such processes. They include both e-signatures and e-records.

This is done so that the legality of the process is affirmed.

2) The commercial acceptance is also another vital condition. This is specified in Article (30/b). The contracting parties should consider the commercial aspects too.

3) The agreement which is reached between the contracting parties can contain the processes the parties think can be applied for a certain transaction. This process can be framed in a way that benefits all the parties involved in performing that transaction. This specified process is in addition to the existing laws which are included in the ETL.

2.2. Conditions of Authentic E-Signature

The Jordanian laws have not specified that the verification is the sole condition that needs to be fulfilled in order to affirm that the e-signatures under consideration are of legal significance. There are other conditions too which have been connected to the verified e-signature which have to be taken into account and then employed as a way of proving the legality of the consent of the party. Article (31) of the ETL contains these conditions.

Article (31) of the ETL gives the following characteristics of a valid signature:

1) It is one of a kind and is related to the correct person and it can easily be differentiated from the e-signatures of other people.

2) The e-signature should be enough for the identification of the person who produced it. Certain measure can be taken to ensure this, but it should be remembered that the signatures themselves must be unique.

3) The e-signatures must be produced and regulated by the rightful owner only and it may only be used by the owner or by a person who is given the authority to use the signature on behalf of the owner. The owner of the e-signature should have exclusive rights for the usage of the e-signature and no other person should be able to produce the e-signature or use it for any person.

4) The e-signatures have to be linked to the e-records with the help of the connection reserved for the purpose. This connection must not be compromised and it should have a direct link to the e-records. If this is not the case, anyone would be able to access the e-signature and they could use it without the consent of the rightful owner. This would make the e-signatures lose validity as the owner would not be in a position to control the e-signature anymore. In this case it would be possible for unauthorized people to produce it and this would lead to the e-signature losing its legal status.

3. Formal/Model Conditions

Jordanian regulations detailing multiple parameters of the authentication certificates, their validity, their relations vis-à-vis the related identification symbols are all detailed in the ETL as per the following:

3.1. E-Signature Should Be Signed within the Validity Period of the Approved Authentication Certificate

All certificates issued have a stipulated validity period, beyond which it would have no

consideration whatsoever if presented anywhere. Correspondingly and similarly, e-signatures too are required to be placed on the document within the designated authentication period to enable the certificate to carry legal weight age, and if the signature is placed and associated with the document beyond such period, there would be value for the same since it would not be fulfilling the objectivity parameters of the e-signature meeting "the authentication condition".

3.2. Authentication Certificate Should Correspond with Identification Symbol

This is related to the requirement for the authentication certificate to correspond with the authentication symbol, so that only the concerned and related can access the contents of the electronic file, and thus the privacy of the text is maintained. This is however, appropriately covered for in Article (34).

To summarize, in the modern day and age, e-signatures are probably extensively utilized across the internet to conclude and finalize agreements and contracts. The maintenance of such electronic records in corresponding databases, however, requires that the legal aspect related to this medium be addressed properly and the legalities involved therein are adhered to in all its entirety, so that agreements concluded incorporating such technological aspects would subsequently stand up for scrutiny in a court-of-law.

However, the writer of the document is under the perception that while modern day legislation like the ETL does address the legal aspects related to e-signatures to a great extent, and the wording of such laws does seem to be cognizant of the multiple aspects required to be covered, however, there are at times probably discrepancies in the way the laws are interpreted during their application in actual situations.

To this end, a number of instances of such discrepancies maybe found in Article (2) of the ETL, which has specified the situations where e-signatures are applicable but falls short on the verification requirements for the same. Further, it could also be observed that the same article has not expressly delineated the parameters of the signatory, although it does sufficiently identify the parameters of the authentication certificate. Stipulations on the required competency of the licensing authorities for the certifications are also an aspect which needs to be further worked upon.

The ETL aspect of Jordanian legislation lays down two parameters for the recognition and validity of e-signatures, which need to be met to enable the same to stand scrutiny in a court of law. These parameters are listed and defined in Articles (7, 10 and 30), and later in Articles (31) and more appropriately in (32/b). In all the above sections, it is emphasized that e-signatures should at all times be authenticated to subsequently withstand legal scrutiny although there are no further explanations and directives on how the authentication process needs to be actually coordinated.

4. Use of E-Signature, "To Prove Contracts Concluded through the Internet"

In addition to the ETL in Jordanian legislation determining and governing the parame-

ters for e-signatures, there are also other related legislatures which shed some further light on this aspect, including UNCITRAL 2001[2], the ECD 1999[3] and the E-SIGN[4]. All of these provide further assistance in determining the legality and related aspects of e-signatures under the laws of the land.

The use of e-signatures on the internet towards executing and entering into a legal binding will be evaluated in three stages. The first will look into the situational parameters of the e-signature, the second will debate upon the duties and responsibilities of both parties entering into an electronic contract, while in the concluding section the legal standing and implications of foreign signatures will be looked into since one of the two parties entering into contracts with foreigners would not be covered under the laws of the land.

4.1. Legal Conditions of E-Signatures, "Conditions That Are Stated under the Selector Laws"

The validity of an e-signature is primarily dependent on addressing two aspects, i.e. the functions to be performed by the signature, and secondly the conditions and parameters under which the signature is provided. However, researchers have determined that there may be discrepancies and shortcomings in the legislation covering the aforementioned aspects[5]. As a general rule, and in essence, e-signatures have been granted the same and equal weight age provided to traditional written signatures[6] as long as both forms of signing off fulfil the standard parameters of signatures[7] (Nsairat, 2005: pp. 126-133; Dodeen, 2006: pp. 260-266; Reed, 2004: pp. 279-285).

The legal standing of e-signatures is, hence, generally governed by two tiers of legalities[8]:

1) When standard functions of a written signature are performed by an e-signature, it is considered as a "general validity in proof"[9] (Dumortire, 2002: pp. 55-57).

2) On a higher level, an e-signature would have the "the validity of a written signature" if the signature so made or presented is able to withstand scrutiny in a court of law without the support of a subsequent written signature[10]. There are perhaps specific technical parameters which need to be addressed before this level is practically real-

[2]Model Law on Electronic Signatures of the United Nations Commission on International Trade Law.

[3]DIRECTIVE 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[4]Electronic Signatures in Global and National Commerce Act.

[5]For more information see: United Nations, "UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001" (United Nations Publication, New York 2002) Online version, 51-57 <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf> accessed 10-10-2015.

[6]United Nations "UNCITRAL" 37-40; National Conference of Commissioners on Uniform State Laws "UETA" National Conference of Commissioners on Uniform State Laws, "Uniform Computer Information Transactions Act, Last Revisions or Amendments Completed Year 2002, with prefatory note and comments" [2002] Annual Conference Meeting in its ONE-HUNDRED-AND-ELEVENTH Year, Tucson Arizona July 26-August 2, 2002, Online version, 81 <https://www.law.upenn.edu/library/archives/ulc/ucita/2002final.pdf> accessed 20-10-2015 19.

[7]The legislations that adopted such method are: the UNCITRAL 1996, the UETA and the E-SIGN.

[8]The legislations that adopted this method are: the UNCITRAL 2001 and the EC Directive 1999/93.

[9]United Nations "UNCITRAL 2001" 52-53.

[10]United Nations "UNCITRAL 2001" 52-53.

ized[11]. (Dumortire, 2002: pp. 55-57)

Researchers do accept that the aforementioned are well in alignment to the definitions and parameters set forth and defined in the existing legislative laws enacted. While some of the laws set the broad parameters to equate e-signatures with the actual written version; others focus more on the specifics and details of e-signatures detailing on such parameters as the integrity, security, confidentiality etc. To consider the relationship between the signatory and the certificate provider, ECD 1999/93 is an illustration of this[12].

Should the signatory desire that the e-signature provided be treated completely at par to that of the traditional written signatures, the following aspects need to be probably fulfilled and kept in consideration[13]:

[11]Ibid, 53.

[12]Based on Article (5/1), which states: "*Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device*: (a) *satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data*; *and* (b) *are admissible as evidence in legal proceedings*".

[13]These conditions provided by the UNCITRAL 2001 within Article (6/3), which states: "*An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph* 1 *if*: (a) *The signature creation data are*, *within the context in which they are used*, *linked to the signatory and to no other person*; (b) *The signature creation data were*, *at the time of signing*, *under the control of the signatory and of no other person*; (c) *Any alteration to the electronic signature*, *made after the time of signing*, *is detectable*; *and* (d) *Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates*, *any alteration made to that information after the time of signing is detectable*"; It should be noted that the UN legislation states illustrative rules in relation to this rule, where Article (6/4) of the UNCITRAL 2001 states: "*Paragraph* 3 *does not limit the ability of any person*: (a) *To establish in any other way*, *for the purpose of satisfying the requirement referred to in paragraph* 1, *the reliability of an electronic signature*; *or* (b) *To adduce evidence of the non-reliability of an electronic signature*"; also, Article (7) of the same law states:" 1. [*Any person*, *organ or authority*, *whether public or private*, *specified by the enacting State as competent*] *may determine which electronic signatures satisfy the provisions of article* 6 *of this Law.* 2. *Any determination made under paragraph* 1 *shall be consistent with recognized international standards.* 3. *Nothing in this article affects the operation of the rules of private international law*". Although, by the EC Directive 1999/93 under Article (2/2) that states: "'*advanced electronic signature*' *means an electronic signature which meets the following requirements*: (b) *it is capable of identifying the signatory*; (c) *it is created using means that the signatory can maintain under his sole control*; *and* (d) *it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable*". It should be noted that the EU legislature provided illustrative rules that determined the qualified certificate within ANNEX I of the EC Directive 1999/93, which states: "*Qualified certificates must contain*: (a) *an indication that the certificate is issued as a qualified certificate*; (b) *the identification of the certification-service-provider and the State in which it is established*; (c) *the name of the signatory or a pseudonym*, *which shall be identified as such*; (d) *provision for a specific attribute of the signatory to be included if relevant*, *depending on the purpose for which the certificate is intended*; (e) *signature-verification data which correspond to signature-creation data under the control of the signatory*; (f) *an indication of the beginning and end of the period of validity of the certificate*; (g) *the identity code of the certificate*; (h) *the advanced electronic signature of the certification-service-provider issuing it*; (i) *limitations on the scope of use of the certificate*, *if applicable*; *and* (j) *limits on the value of transactions for which the certificate can be used*, *if applicable*"; although, it's determined secure-signature-creation devices under ANNEX III of this Directive that states: "1. *Secure signature-creation devices must*, *by appropriate technical and procedural means*, *ensure at the least that*: (a) *the signature-creation-data used for signature generation can practically occur only once*, *and that their secrecy is reasonably assured*; (b) *the signature-creation-data used for signature generation cannot*, *with reasonable assurance*, *be derived and the signature is protected against forgery using currently available technology*; (c) *the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.* 2. *Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process*".

1) The signature in question should be uniquely linked to the person providing it, i.e. the "signatory"[14].

2) The characteristics of this e-signature should be such that it is uniquely possible to identify the signatory through the signature[15].

3) The signature provided should be in a manner so that the form and design of the same is not subsequently altered, like that of the written signature[16].

4) The signature provided against a certain text be so linked to the entire document so that all aspects of the particular page remain unaltered and could not be tampered so that the originality of the entire page and the signature provided is retained, and "any alteration is detectable".

Considering all the above, it is to be concluded that if an e-signature is able to fulfil the stipulations and aspects described, it can definitely be considered to have the same standing in any legal framework just as the traditional written signature, and would be surely considered as an "advanced, enhanced or authentic e-signature".

The researchers have also had occasion to specify and identify certain anomalies with respect to e-signatures in the perception and understanding of Jordanian legislators drafting and finalizing the related text of such laws, including the ETL. Perhaps, some of these aspects could be:

- While Article (2) of the ETL does provide a general definition and overview of what are e-signatures, it unfortunately fails to provide specifics on the authentication process of the same.
- Article (10) only goes to specify the general parameters of the e-signature validity aspect, describing the basic functions of the same.
- Article (30) lists the authentication process while Article (31) specifies the conditions and situations under which such signatures would be considered to be valid.
- Article (32/b) of the ETL lists "the confusing rule" whereby it is mandatory that the authentication process and parameters must be fulfilled for e-signatures to ensure that they subsequently remain valid over the long run.

As per all the above descriptions, the authors would conclude that the ETL covers for validating e-signatures only where the same is authenticated, and correspondingly viewing the same under the lens of Article (10) of the ETL would strip away any legal coverage for unauthenticated e-signatures. However, this stance projected is perhaps a bit misleading since other aspects do not reflect and support this. It must be kept in perspective that technological advances and progress in such related aspects as encryption technology and the like has already provided sufficient coverage to authenticate e-signatures under all the stated parameters, and is surely compliant with being able to provide authentication processes for signatures "as legal conditions".

Considering the above, the authors are of the perspective that Jordanian legislation should do all the needful so that the current ambiguities in legislation enacted such as the ETL is not in conflict with other aspects of the law related to this sphere. Laws en-

[14]United Nations "UNCITRAL 2001" 54.

[15]Ibid.

[16]Ibid.

acted should all be in perfect synchronization and harmony to each other, and should supplement and complement each other. As pointed out for Article (3) in the aforementioned text, it would be detrimental to have such ambiguity in the Jordanian legislation process.

The issue of the legality of e-signatures has also been dealt with through the judicial systems, as demonstrated in the processes of the US judicial systems, where this aspect was appropriately addressed since the remaining aspects of the functions and conditions of the same were already appropriately defined[17] (Moringiello & Reynolds, 2005: p. 433).

4.2. Conducts and Liabilities Resulted from Use of E-Signature

The authors are of the learned opinion that the ETL fails to address the issue of the obligations and any requirements whatsoever upon the contract parties entering into an agreement through an e-signature. Similar legislation enacted including UNCITRAL 2001 and ECD 99/93, however, does provide so, and lists certain obligations on both the parties, which includes the signatory, the relying party and even the certification provider, as depicted by the following:

4.2.1. Conducts of Signatory

This liability is stated by the UNCITRAL 2001 under Article (8/1). According to this rule, the signatory shall:

"… (a) *Exercise reasonable care to avoid unauthorized use of its signature creation data;* (b) *Without undue delay, utilize means made available by the certification service provider pursuant to article* 9 *of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if*: (i) *The signatory knows that the sig-*

[17]To determine the validity of e-signature in proof, these cases (from USA courts), as examples, will illustrate how the U.S judicial system dealt with such subject:

(a) In, *Kerr v. Dillard Store Services*, [2009] Dist. Court, D. Kansas, the court found the protection of e-signature simply was not enough. As, the employer "did not have adequate procedures to maintain the security of intranet passwords, to restrict unauthorized access… to determine whether electronic signatures were genuine or to determine who opened individual e-mails". The result from this case was if the party wanted to rely on an e-signature he/she should ensure that this signature is valid.

(b) In *Riensche v. Cingular Wireless, LLC* [2006] *Dist. Court, WD Washington* 2007, the court held that Riensche was bound by its terms, because Cingular proved that Riensche was required to click to agree to the terms before receiving his service, for this evidence Cingular proved that Riensche signed the terms and thus was bound by these terms; according to e-contracts statutes (UETA S.2/8 and E-SIGN S.7006/5), a click qualifies as a signature.

(c) In *CSX Transportation, Inc. v. Recovery Express, Inc* case, according to the official comment 7 of the UETA S.2, a person name in an e-mail communications can suffice as a signature if that person whose name appears in the e-mail has the intent to sign the record. In this case CSX argued that basing on the e-mail address, "albert@recoveryexpress.com", and by giving Arillotta an e-mail address in the recoveryexpress.com domain, Recovery Express had granted Arillotta apparent authority to transact business on its behalf. This argument was rejected by the court, and noted on CSX's argument that "every subordinate employee with a company e-mail address-down to the night watchman-could bind a company to the same contracts as the president". The court in this case chided CSX for basing on such kind of signature; where CSX instead should have requested a more reliable form of authentication in such a case.

nature creation data have been compromised; or (ii) *The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised*; (c) *Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate*".

The UNCITRAL 2001 provided that these conducts shall be the responsibility of the signatory, as Article (8/2) states:

"*A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph* 1"

4.2.2. Conducts of Certification Service Provider

As per Article (9)[18] of UNCITRAL 2001, the certification service provider has certain duties and obligations to fulfil, and any shortcomings and failure in executing upon those assignments would make the service provider legally liable to make good on the discrepancies subsequently detected.

[18]As, Article (9) states: "1. *Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall*:

(a) *Act in accordance with representations made by it with respect to its policies and practices*; (b) *Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate*; (c) *Provide reasonably accessible means that enable a relying party to ascertain from the certificate*:

(i) *The identity of the certification service provider*;

(ii) *That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued*;

(iii) *That signature creation data were valid at or before the time when the certificate was issued*;

(d) *Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise*:

(i) *The method used to identify the signatory*;

(ii) *Any limitation on the purpose or value for which the signature creation data or the certificate may be used*;

(iii) *That the signature creation data are valid and have not been compromised*;

(iv) *Any limitation on the scope or extent of liability stipulated by the certification service provider*;

(v) *Whether means exist for the signatory to give notice pursuant to article* 8, *paragraph* 1 (b), *of this Law*;

(vi) *Whether a timely revocation service is offered*;

(e) *Where services under subparagraph* (d) (v) *are offered, provide a means for a signatory to give notice pursuant to article* 8, *paragraph* 1 (b), *of this Law and, where services under subparagraph* (d) (vi) *are offered, ensure the availability of a timely revocation service*;

(f) *Utilize trustworthy systems, procedures and human resources in performing its services.*

2. *A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph* 1". See: United Nations "UNCITRAL 2001" (n287) 64-65.

Although, Article (10) of the UNCITRAL 2001 determines where the systems are trustworthy, by stating: "*For the purposes of article* 9, *paragraph* 1 (f), *of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors*:

(a) *Financial and human resources, including existence of assets*; (b) *Quality of hardware and software systems*; (c) *Procedures for processing of certificates and applications for certificates and retention of records*; (d) *Availability of information to signatories identified in certificates and to potential relying parties*; (e) *Regularity and extent of audit by an independent body*; (f) *The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing*; or (g) *Any other relevant factor*". See: United Nations "UNCITRAL 2001" (n287) 66.

Under Article (6)[19] of the ECD 99/93, there are unambiguous directives for the certification service provider to ensure that the level and standard of certification provided has to stand up to public scrutiny at any subsequent public evaluation and analysis of the certification so provided. In this regard, EU legislation has provided ample directives on the certification provider and the same would be detailed in ANNEX II of the ECD 99/93[20]. (Dumortire , 2002: pp. 57-59).

[19]As, Article (6) states: "1) *As a minimum*, *Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate*: (a *as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate*; (b) *for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate*; (c) *for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both; unless the certification-service-provider proves that he has not acted negligently.* 2) *As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.* 3) *Member States shall ensure that a certification-service-provider may indicate in qualified certificate limitations on the use of that certificate. Provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.* 4) *Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties. The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.* 5) *The provisions of paragraphs* 1 *to* 4 *shall be without prejudice to Council Directive* 93/13/*EEC of* 5 *April* 1993 *on unfair terms in consumer contracts*".

[20]Thus, ANNEX II states: "*Certification-service-providers must*: (a) *prove the reliability necessary for providing certification services*; (b) *ensure the operation of a prompt and secure directory and a secure and immediate revocation service*; (c) *ensure that the date and time when a certificate is issued or revoked can be determined precisely*; (d) *verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued*; (e) *employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards*; (f) *use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them*; (g) *take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature creation data, guarantee confidentiality during the process of generating such data*; (h) *maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance*; (i) *record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically*; (j) *not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services*; (k) *before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate*; (l) *use trustworthy systems to store certificates in a verifiable form so that*:

—only authorised persons can make entries and changes,

—information can be checked for authenticity,

—certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and

—any technical changes compromising these security requirements are apparent to the operator".

4.2.3. Conducts of Relying Party

These kinds of conducts[21] are stipulated under the UNCITRAL 2001, in Article (11). The rule of this Article states:

1) *"A relying party shall bear the legal consequences of its failure:*

2) (a) *To take reasonable steps to verify the reliability of an electronic signature; or*

3) *(*b) *Where an electronic signature is supported by a certificate, to take reasonable steps:*

4) (i) *To verify the validity, suspension or revocation of the certificate; and*

5) (ii) *To observe any limitation with respect to the certificate".*

The authors do notice that the legalities of this particular aspect has also been sufficiently and to a great extent covered under Article (33) of the ETL too. However, the coverage provided under existing Jordanian laws is deemed too generalized, and should be far more specific and detailed so that it would stand up to close legal scrutiny and review. Perhaps, a specific aspect requiring additional input would be contracts signed over the internet where international signatories would also be very well involved.

Considering all the above, it is quite clear that Jordanian legislation should take the necessary steps towards ensuring that the gaps and loopholes in existing laws, including the ETL are all resolved and done away with at the soonest, so that there are minimal issues with e-signatures in the future, and agreements entered into and concluded by individuals through e-signatures; all stand up to legal scrutiny and evaluation.

4.3. Recognition of Foreign Signature and Certificate

It is observed that the legalities and specifics of recognizing foreign e-signatures are dealt with under Article (12) of UNCITRAL[22]. Similarly and correspondingly, Article (34) of the ETL and Article (7/1)[23] of ECD 99/93 have also stipulated the specifics in dealing with this aspect (Dumortire, 2002: pp. 57-59).

[21]For more information see: United Nations "UNCITRAL 2001" 76-77.

[22]Whereas, Article (12) states: "1. *In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had*: (a) *To the geographic location where the certificate is issued or the electronic signature created or used*; *or* (b) *To the geographic location of the place of business of the issuer or signatory.* 2. *A certificate issued outside [the enacting State] shall have the same legal effect in* [*the enacting State*] *as a certificate issued in* [*the enacting State*] *if it offers a substantially equivalent level of reliability.* 3. *An electronic signature created or used outside* [*the enacting State*] *shall have the same legal effect in* [*the enacting State*] *as an electronic signature created or used in* [*the enacting State*] *if it offers a substantially equivalent level of reliability.* 4. *In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph* 2 *or* 3, *regard shall be had to recognized international standards and to any other relevant factors.* 5. *Where, notwithstanding paragraphs* 2, 3 *and* 4, *parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law*". See: United Nations "UNCITRAL 2001" 69-72.

[23]Article (7/1) states: "*Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if*:

(a) *the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member state*; *or* (b) *a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate*; *or* (c) *the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations*".

As per the observations made after the detailed analysis and evaluation undertaken in this study, the authors of this article would recommend that Jordanian legislation should perhaps bring about the necessary and required modifications in existing laws like the ETL to ensure that foreign input on e-signatures is fully governed, and the laws are in harmony with global standards already formulated in this aspect, "especially the simple signature". Jordanian regulations should also elaborate on certain specific signatures, such as those listed in UNCITRAL 2001, so that contracting parties could keep them in perspective too while entering into national and international contracts through e-signatures. All this would go towards ensuring that individuals entering into contracts are facilitated to the extent possible, and there are minimal problems in understanding any ambiguity in the agreement which could possibly turn up at any time in the future.

5. Conclusions

The authors are of the opinion that numerous aspects of e-signatures are further elaboration, which is perhaps not provided so by the existing state of the ETL. These could include aspects of the definitions of e-signatures, their validity, the corresponding authentication certificate and recognition of foreign certificates etc.

The authors are of the opinion that while the ETL has defined e-signatures in Article (2), but there are certain shortcomings in this respect regarding how such signatures would be deemed to be authentic and genuine. Perhaps this aspect is addressed in other aspects of the current legislation enacted, but it should be unambiguous in this respect.

As per Article (2) of the ETL, while the authentication certificate has been probably partially defined, the signatory too needs to be legally defined and elaborated upon. The legislation should also elaborate upon the required certifications and identify the acceptable licensing and certifying authorities for this purpose.

A major issue highlighted and appropriately discussed in the subsequent text is regarding the parameters identifying an e-signature and authenticating the same. The current form of the ETL provides for two different ways for verifying e-signatures, which at times creates ambiguity. Thus, Articles (7, 10 and 30) and Articles 31, and specifically 32/b need to be synchronized and aligned with each other so that they supplement and complement each other instead of creating ambiguities. In its current form, the rules and their different interpretations could have the unfortunate effect of cancelling out and delegitimize e-signatures while concluding any agreement using this aspect.

Towards resolving the various loopholes and issues identified in this article, the authors are of the opinion that Jordanian legislatures need to go for a minor overhaul of the existing laws. This could be in the form of not just redefining e-signatures in general, but also making a proper definition of an authentic e-signature. The laws also need to elaborate and define on certificates and the competent licensing authorities for these certificates. Aspects of authentication certificates provided and issued also need to be addressed and worked upon. All the above changes and additions to the existing laws

would certainly go a long way towards ensuring that legal loopholes and ambiguities are removed to the extent possible.

As a result, the recommended definitions, based on the rules provided under the UNCITRAL 2001 and the EC Directive 99/93, "borrowing", of these subjects are:

- An e-signature means: "*Data in electronic form or similar means which is attached to, or logically associated with a data message or an e-record, which is used as a method which identifies the signatory in connection with that message or record, and to indicate the signatory's approval of the information contained in the data message or e-record*".
- An authentic signature means: "*An e-signature that meets the requirements laid down in Article* (31) *of this law*".
- A signatory means: "*A person who holds a signature identification symbol and acts either on his behalf or on behalf of a natural or legal person or entity he represents*".
- A certificate means: "*A data message or e-record or other e-means that confirms the link between the signatory and signature identification symbol*".
- An authentication certificate means: "*A certificate provided by the competent licensing authority, and which contains the following requirement*: (here the legislation can adopt the requirements provided by the ECD 99/93 in ANNIX 1)".
- A competent licensing authority means: "*An entity or legal or natural person who issues certificates or provides other services related to an e-signature or e-record, which meets the requirements laid down in Articles* (30 & 31) *of this law*".

Perhaps, the major anomaly, loophole and shortcoming of the ETL in its current form lies in its definitions regarding the validity of e-signatures and the authentication of e-signatures when placed on a document, so that the agreement would subsequently stand up review in a court-of-law. Hence, it is very important that the laws be appropriately amended to enable for e-signatures to be at par to traditional signatures, while they should have the same standing in a legal document to that accorded to a written signature. Towards this end, the authors are of the opinion that the existing wording of Article (32/b) need to be changed and amended, so that they are made to read as "… *it shall not be deemed qualified as a written document or signature in evidence thereat*" instead of the current "… *it shall not have any legal effect*".

References

DIRECTIVE 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.

Dodeen B. (2006). *The Legal Firm of the Concluded Contract through the Internet* (1st ed.). Amman: Althaqafa Publisher.

Electronic Signatures in Global and National Commerce Act.

Electronic Transaction Law No. (85) of 2001.

Model Law on Electronic Signatures of the United Nations Commission on International Trade Law.

Moringiello J. M., & Reynolds W. L. (2005). Survey of the Law of Cyberspace: Electronic Contracting: Cases 2004-2005. *Business Lawyer, 61,* 433.

http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=juliet_moringiello

National Conference of Commissioners on Uniform State Laws "UETA" National Conference of Commissioners on Uniform State Laws, "Uniform Computer Information Transactions Act, Last Revisions or Amendments Completed Year 2002, with prefatory note and comments" [2002] Annual Conference Meeting in its One-Hundred-and-Eleventh Year, Tucson Arizona 26 July-2 August 2002, Online Version, 81.
http://www.uniformlaws.org/shared/docs/mediation/uma_final_03.pdf

Nsairat, A. (2005). The Legality of E-Signature in Proof (1st ed.). Amman: Althaqafa Publisher.

Reed C. (2004). Internet Law (2nd ed.). Cambridge University Press.

United Nations (2002). *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001* (pp. 51-57). New York: United Nations Publication, Online Version.
http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf