The Civil Liability of the Authentication Authority in Accordance with the Emirate Electronic Transactions & Commerce Law

Dr. Yousef Ahmad Nawafleh
Al Ain University of Science & Technology
Private Law Department

Abstract

After presenting the introduction and the problem, this study examined the civil liability of the electronic authentication provider in accordance with the UAE Electronic Transactions & Commerce Law No. (1/2006). In the first chapter, the study spotlighted the definition of the electronic authentication as well as the authentication authority which is authorized to issue the relevant licenses for the provider. It also demonstrated the procedure of obtaining licenses by the electronic authentication provider. Moreover, the study discussed the definition of electronic authentication certificate, the conditions that should be met by the provider and its obligations in accordance with the UAE Electronic Transactions & Commerce Law No. (1/2006) and the UAE Resolution No. (1/2008). In the second chapter, the study examined the civil liability of the electronic authentication provider in accordance with Article No. 21/4 thereof and The Civil Transactions Law too. The researcher differentiated between the two types of the civil liability, namely; the contractual liability and tort liability which obliged the electronic authentication provider to compensate as a result of its default and failure to commit with its obligations and liabilities either contractual or tort. Additionally, the study discussed the cases when the provider is not responsible for compensation for damages as a result of its failure and default in fulfilling its obligations or liabilities per sue the law or contract either contractual or tort in accordance with Article No. 21/5 thereof and Article No 282 of the UAE Civil Transactions Law. The study also demonstrated the case through with the provider can exempt itself from offering any compensation for its contractual liability and tort liability such as providing evidence of a foreign reason or force majeure or the act of the prejudiced itself. Finally, the study concluded that the electronic authentication services provider should shoulder the civil liability either contractual or tort along with taking into account the recommendations of the study represented in the importance of paying attention to the conditions as well as to consider that the contractor or uninjured party might not have complete knowledge of the terms and conditions of the contract since the provider had the experience in this domain and in order to protect the contractor or others from being cheated or manipulated by the provider specially if the provider is a foreigner in order to take into account the customer's rights and interests and ways of protecting it from any conditions in the contract which discharges the provider from its liability.

Key Words: evidence-based practice; evidence-informed practice; outcome measures; self-assessment.

1. Introduction

The world has witnessed dramatic and unprecedented evolution and development since mid-nineties in the field of Information Technology. Computer technology emerged in late seventies but it developed quickly and noticeably in mid-nineties of the previous century and at the advent of the new millennium and among these developments that the globe has witnessed is the rapid development in the field of digital information technology and e-signature. The e-commerce has also witnessed more development and new governmental e-services have been introduced, Nawafleh, et al, 2012.

Therefore, many countries enact new laws and regulations to regulate and legalize e-transactions and e-signatures including e-authentication service and e-commerce providers and the Arab countries such as the United Arab Emirates which has participated in rapid development in these fields and enacted local laws and regulations, such as Dubai Emirate Law in 2002, the Federal Law No. (1) Issued in 2006 concerning e-transactions and e-commerce.

The United Arab Emirates has witnessed a clear and tangible progress in this area on both the Arab countries and the world levels and all government transactions in the facilities of the State have been computerized and transactions were directly linked with the public and the services applicants. The United Arab Emirates has recently completed e-government project and achieved qualitative shift towards electronic commerce, transactions and signature. The United Arab Emirates has issued regulations which govern the work of electronic authentication services providers per sue Ministerial Decree No 1 issued in 2008 as an important part in the enforcement of Federal Transactions Law, trade as a main and important within the context and framework of the completion of e-commerce transactions and e-signature, which is third party in the deal occurs between distant parties and who often do not know each other therefore, the provider e-commerce services is the party that is trusted by the parties of the transactions in order to complete them securely and trustfully.

Study Problem

That electronic authentication services provider like any service providers in any field may commit errors or fault in the systems whether this contractual error result in contractual relationship or omissive fault towards third parties of non-contractual parties. Such fault or system malfunction or non-observance of laws, regulations and requirements in effect in the United Arab Emirates also may occur, therefore it necessary to take into account such errors and faults that may take place and to demonstrate the provider's responsibility is such conditions in the event of a defect, malfunction, error or failure to follow the terms of the licensing laws and regulations in force upon the license was issued to the service provider issued or failure to observe the terms of the agreement concluded with the provider. The study addressed and highlighted the contractual and missive responsibility of authentication service provider and scope of this responsibility briefly as well as cases which services provider shall not assume the responsibility for these errors and therefore for compensation in the cases cited by Electronic Transaction & Commerce Federal Law as well as the general rules contained in the UAE Civil Transactions Law, after reviewing the definition of authentication services provider as set out in the Act and the Regulations and jurisprudence and authority which grant licenses in addition to its conditions and authentication mechanism.

Requirement Number One: Definition of e-authentication and its competent authority

Article 2 item no. 1 of the Electronic Transaction & Commerce Federal Law defines the electronic Certificate of Authenticity "the certificate issued by the authentication services provider which confirms identity of the person or entity possessing a certain signing tool". The Emirati legislator defines in the same article authentication services provider (someone or an accredited or recognized authority which issues electronic authentication certificates or any services or relevant tasks and electronic signatures that are regulated under the provisions of this law). Article 1 of electronic authentication services providers' regulations define under Ministerial Decree No. (1/2008) in explaining authentication as (a statement issued by the electronic authentication services provider in order to challenge the practices and procedures employed by electronic authentication provider in issuing of electronic authentication certificates and digital key with respect to electronic signatures and any other licensed services).

The jurisprudence also defines the electronic authentication service provider as (any natural or legal person who issues electronic certificates and provides other services related to electronic signatures and ensures the identification of the contracting parties and retains these data and information for a certain period and commits to respect the regulatory rules its work and which are determined by the competent authority[1]) Under the Emirati Council of Minister's decision non (291/8) in its session held on October 15th, 2006 Telecommunications Regulatory Authority was appointed the as an observer for electronic authentication services to license, certify and monitor the activities provided by authentication services providers as well as Ministry of Economy which shall assume its supervisory role according to the provisions of the law, so that the Telecommunications Regulatory Authority is the supreme authority of authentication in the UAE which grants the necessary license to authentication authorities to carry out their works in United Arab Emirates, that issues licenses to provide electronic signature services. The Telecommunications Regulatory Authority has actually granted such licenses after the announcement of the conditions required under the provisions of article no. 21 of the same law and four companies were granted license to practice the activity of electronic authentication services in the UAE.

[1] The Civil Liability of authentication services providers according to the Syrian jurisprudence, M. Nafan Satas. Available in the following website: ***http://syrianbar.org*** .

Authentication Authority

The endorsement of the third person on the secured e-signature is a job which appeared as a result of the development of the Internet network and to guarantee the security of the e-signature and e-correspondences. As we mentioned earlier the Telecommunications Regulatory Authority which follows the Ministry of Economy is the competent authority which assume the responsibility of providing licenses for authentication authorities and one of its important goals is to regulate electronic authentication services and e-signature activities in the field of e-transactions and e-signature. It is also the supreme competent authority to issue, renew or cancel licenses to carry out e-signature authentication services as well as their system and specifications, evaluation of authorities which provide such services and receive complaints in this regard. The Ministerial decision number 291/8, upon which the regulations of electronic authentication services provider, also clarified that the Telecommunications Regulatory Authority assumes the responsibility of supervising electronic authentication services in the UAE as well as the mechanisms of issuing licenses for parties who provide e-signature services in addition to the technical and technological specifications related to the work and activities of those parties and the specification, regulations and rules that shall be met by such parties to carry out their activities in this domain[2]. The task of the entity or body authorized and licensed by the Telecommunications Regulatory Authority and which has been duly certified and licensed shall submit authentication or certification certificate to the entity which demanded it and under this certificate any party can verify that the public and private key, which contains the editor and electronic signature, belonging to the party who sent the these data and the signature –i.e. for the first sender party - and this is based on the entity which is authorized and licensed to verify through its work system from personality of the subscriber and then the Telecommunications Regulatory Authority the authentication party shall grant the requester the e-authenticated certificate[3].

Item Number One: Procedures of obtaining authentication licenses[4]

The resolution of electronic authentication service providers showed the terms and conditions that shall be met by companies and are applicable to both all those who provide electronic authentication services. This resolution also specified the documents that shall attached to the license application as set forth in Article number 3 of the Regulations. and the Telecommunications Regulatory Authority asked fill out the special form in order to obtain a license electronically or by mail and explaining in the application form the information on the applicant and the capital of the entity which request authentication as well as the commercial registration number, address and type of company, authorized its phone number, e-mail and previous experience in this area and experience in the field of information technology and the fees that shall be paid to obtain the license. After submitting stated requests of the Ministry of Economy and the Telecommunications Regulatory Authority accompanied by the required documents such as commercial register certificate and application fee then the Telecommunications Regulatory Authority shall issue its decision concerning the application for approval or rejection and the Authority has identified specifications that shall be met by these companies and the technology used which a system based on, Public Key and Private Key.

---

[2] Article 20 of the Electronic Transaction & Commerce Federal Law stipulates (for purposes of this Law) upon the a decision made by the Council of Ministers, a supervisory shall be appointed to supervise authentication services providers, in particular for the purposes of licensing, approval and monitoring and supervising of the activities carried out by the authentication service providers). Article 22 of the same law also stipulates the (the minister shall issue upon the observer's proposal regulations related to the regulation of licensing the work of authentication services providers who practice their work in the UEA, including the following:

Licensing, renewing the licenses of authentication services providers and their delegated representatives as well as renewing these licenses and their relevant issues.

Authentication services providers' activities including the method, place and the way of obtaining their work and attracting the public.

Standards and rules that shall be met and maintained by the authentication services providers and they shall observe when carrying out their businesses.

Challenge suitable standards pertain to the qualifications and experiences of authentication services providers and the train of their personnel.

Specification of the terms and conditions of business management carried out the authentication services providers' activities.

[3] Dhya' Mushmosh, The Electronic Signature, Comparative Study of the Legal Publications. Issued in 2003 P. 165 et seq. Eng. Omar Al-Monani, The Electronic Signature and the E-Commerce Law, Dar Wa'el for Publication, 2003 P.P. 62 – 63.

[4] They are available on the following website of the Telecommunications Regulatory Authority in the United Arab Emirates: ***http://www.tra.gov.ae/ar*** **.**

And the need to use the of security means for these keys through using reliable technology, taking into account the reliability of the computer software, hardware and procedures for processing and issuing of certificates that are electronically authenticated as well as applications for obtaining certificates and maintaining records as set out in Article 21 of the Electronic Transaction & Commerce Federal Law.

The Telecommunications Regulatory Authority has identified the license period for these companies which is five years for local companies and one year for foreign companies starting from the date of issuing operation permit for these companies by the Authority. These companies can't exercise their business activities before the issuance of this authorization. The Authority has also identified license fee for each company which amounts to seventy-five thousand dirham (AED 75,000) per year from the date of issuing of the operation permit. The provider shall also possess financial sources that shall not be less than five millions dirham (AED 5,000.000) for the duration of the license validity which shall be insured against any financial loss[5]. Services offered by these entities shall be in accordance with the instructions issued by the Telecommunications Regulatory Authority and available to work 24 hours round week. The Authority shall also provide the licensed company the private root key cryptography of the user from the licensee to develop electronically authenticated certificates and the data used for creating electronic signature.

The Telecommunications Regulatory Authority has the right under the provisions of Article 10/22 of the Electronic Transaction & Commerce Federal Law and Article 9 of Regulations to evaluate the licensed companies and review their work and carry out periodic inspections to ensure compliance with the aforementioned licensing and operation conditions, and it also has shown in regulation the standards and requirements of the inspection and audit[6].

Item Number Two: Electronic Authentication Certificate

Article No. (1) Of the Federal Transactions Law defines the electronic authentication certificate as the following "The certificate issued by the authentication service provider which it confirms the identity of the individual or the party which has certain signature tool). It is noticed from the definition that the electronic authentication certificate performs the required job represented in proving the relationship of the e-signature of the signee through relying on authentication procedures that the entity which issued the certificate had approved the e-signature of that person.[7]

The party which issues the authentication or certification certificate shall verify the signee who wishes to authenticate its signature, and the conclusion the contract adopted by the Telecommunications Regulatory Authority with it so shall submit all data relating to it and its commercial and record, if any, certificate, and the Authority verifies the system used in creating the e-signature and then it documents it, and allows Public Key Code to be used on the network and provides it with the Private Root key Cryptography saved on the smart card number and its Personal Identification Number "PIN"[8].

The authentication party shall, upon the request of any interested party and against a fee give electronic signature authentication certificate of the signee, and shall ensure this certificate that is provided by licensed authentication party that the Public Key and Private Key are linked with the site only and that this e-signature shall be valid during the validity period of the certificate. In accordance with Article 21/c of the Electronic Transaction & Commerce Federal Law, the authentication certificate shall includes the following data and information:

1. The identity of the authentication service provider.

[5] Article No. (8/C, D) of the Resolutions stipulates that "C. The applicant shall own financial resources which amount to five million dirham. D. The applicant shall be insured against any financial losses...)

[6] Article number 22/4 of the Electronic Transaction & Commerce Federal Law stipulates the (putting of the necessary conditions for regulating of inspection and audit of the service providers' work activities) and Article no. 9 of the Regulation stipulates the following: The electronic authentication provider shall be subjected to audit and inspection process in accordance with the standards set out in Article no. 9 this regulations and other standards issued by decision made of the Minister based on the proposal of the observer in the following cases:
When submitting the license application for the first time.
Every two years from the date of the license.
When applying for license renewal.

[7] Dr. Tamer Al-Demyati – Proving E-contracting via the Internet – Comparative Study – Edition No. 1, 2009

[8] Dr. Tamer Al-Demyati – Proving E-contracting via the Internet – Comparative Study – Edition No. 1, 2009

2. The person whose identity is concerned with the electronic authentication certificate has the control in the specified time over the signature tool referred to in this certificate as well the serial number of the certificate.
3. The method used in specifying the signee's identity.
4. Presence of ay limitation on the purpose or value that signature tool may be used for.
5. Whether the signature tool is correct and it didn't expose to what might evoke suspicion.
6. Whether the signee has a means to give notification under this law.
7. Whether there is a suitable way to inform about the cancellation of the signature.

After the issuance of certification or authentication certificate, the signee may create the Private Cryptography Key through the Public Cryptography key that was given to it by the authentication authority. This Private Key shall be kept in the non- irreproducible smart card and the site takes it, and it desires to send an encrypted message using the Public Key it shall attach its e-signature on the electronic editor and received by the other party, "the recipient", who sends a copy of the electronic signature sender to the authentication authority in the event of dealing for the first time with the sender –which issues authentication certificate which shall, through the database as well as the system, make sure that the electronic signature of the signee and to inform the recipient with the result whether the e-signature is the signature of the sender or not[9].

The authentication authority has to keep the secrecy and protect the Private Key and provide guidance to its dealers about the way of creating e-signature and using it as well as clients' personal and private life[10]. It is clear from the foregoing that the authentication certificate or electronic authentication of e-signature is important and a definite guarantee for people who want to deal with the signee, and ensures the achievement of important jobs, mainly confidentiality, integrity and reliability which can be achieved by signature in general and the e-signature through using digital signature technology with its Public Key and Private Key and associated smart card that are registered at the authentication party which shall assume the responsibility of e-signature for the duration of the authentication certificate that it issued for the signee.

Requirement Number One: The civil liability of the electronic authentication services providers

Article no. 21, item no. four of the Electronic Transaction & Commerce Federal Law stipulates that (if any damages occurred a result of the incorrectness of the electronic authenticated certificate or due to any fault then the electronic authentication services provider shall shoulder the responsibility towards losses that it incurred as follows:

A- Each party that concluded a contract with the electronic authentication services provider regarding the offering of the electronic authenticated certificate.
B- Any person depended reasonably on electronic authenticated certificate issued by the electronic authentication services provider)[11].

It is noted that the legislator differentiated between the two cases in the text, namely a situation where the person conclude a contract with the same provider about the same benefit from the provider's authentication services and in second case where the third party depends on the authentication certificate issued by provider.

This means that the legislator differentiated between liability for damages that arise between the contractor and provider with a situation where the aggrieved person a third party is not a contractor with provider, but it relied on the certificate issued by the provider.

---

[9] Eng. Omar Hassan Al-Momani, previous resource, P.P. 66 – 69.

[10] Dhya' Mushmosh. A previous resource pages 66 – P.167.

[11](Article 17 of the regulation also stipulates the obligations that shall be assumed by electronic authentication services provider namely:
Electronic authentication services provider shall commit to provide of its service, including the following:
Carrying out business with integrity, credibility and experience in the context of all the activities and business.
Taking into account to be cautious when issuing electronic authenticated certificates for each authorized signatory.
Maintaining trustworthy complete and accurate records for each issuance, renewal, suspension or revocation of electronic authenticated certificates.
Taking the necessary measures and procedures to ensure that the persons entrusted know all the technical developments and the systems and processes related to its business
Maintaining the security standards of its systems and everything related to its input, data and information.
Complying with the standards, conditions and instructions issued by the observer in accordance with the provisions of the law and this regulation).

Item Number One: Liability towards damage that result in the contractual relationship with the provider (The Contractual Liability)

It is the liability that arises from the violation of the contractual obligation and article no.125 of the Emirati Civil Transactions Law defined it as follows: (the contract that is concluded positively by one of the contractors through accepting the other and their agreement in a way which shows its effect on the contracted upon and as a result each of them shall comply with what is imposed on the other party and more than two wells may conform to produce the legal effect).

The following contractual responsibility conditions shall be provided to say that contract is valid and doesn't entail any violations, namely:

1. There is of a valid contract between the contracting parties (the contractor and provider) and if is void or incorrect then there shall be no liability.
2. The contractual liability shall be between the two parties of the contract and not between the provider and a third party because the third party or others can refer to the provider –as we shall explain in the second item – based on the rules of tort liability.
3. The damage caused to the Contractor has resulted in the provider's violation of contract or in executing it defectively.

In the case set out in item four or article no. 21, that there is natural or legal person who contracts with the provider to take advantage of the certification service provided by the supplier then the responsibility between the two parties shall be a contractual liability. If the damage incurred by the contractor with the provider as a result of the invalidity of the given certificate to the contractor due to the existence of any defect then the provider shall in accordance with the general rules contained in the Civil Transactions Law and the text of article no 4/21 of Transactions Law be liable for compensating the contractor against incurred or it may incur as a result of the damage and if there is no agreement in the contract to determine the amount of compensation then the judge shall estimate the compensation due to aggrieved contractor with the assistance of experts in this field and the compensation shall be equal to damage and loss of earnings incurred by the contractor as a result of service provider's fault[12].

Article no. 246 of the Emirati Civil Transactions Law stipulates the following:

1. The contractor shall be executed according to its contents and in accordance with good faith.
2. The contract is not limited only to oblige the contractor of its contents but it also addresses its requirements per sue the law.

In case the service provider doesn't execute the contract according to its contents because of failure to fulfill the obligation resulting from the need to issue authenticated and valid certificate which is free from defects and in conformity with the provisions of the Emirati Electronic Transaction & Commerce Federal Law that have already referred to in Article 21 of the same law.

Therefore, this violation in the execution of the contract or its implementation inconsistent with good faith so that the provider didn't make the necessary diligence to issue of certificate in accordance with necessary legal requirements or the provider has a defect in its business system as if these systems have a defect, untrustworthy, it did not exercise reasonable care and diligence when issuing the certificate, the certificate processing procedures and issuance were not trustworthy or other than stated in the law and the resolution then this defaults shall constitute a breach to the contract with the contractor and in this case the execution of the contract have been done differently to what has been agreed upon or required by good faith. Consequently, the provider shall be responsible for the damage incurred by to the contractor who shall be compensated as a result of this damage[13].

The contractor shall prove the bedrocks of the contractual liability to be able claim for compensation, namely: proving provider's fault and the damage it suffered from and its causal relationship.

[12] Dr. Tamer Al-Demyati – previous resource, page 506.

[13] Dr. Tamer Al-Demyati – previous resource, page 506 et siq.

Item Number Two: Liability towards damage incurred by others (The Tort liability)

Article no. 21/4/B of the Emirati Electronic Transaction & Commerce Federal Law stipulates that (if any damage occurred as a result of the invalidity of the electronic authenticated certificate or because of the any defect then the authentication services provider shall be responsible for the incurred losses: B) Any person depended reasonably on electronic authenticated certificate issued by the electronic authentication services provider.
Article no. 282 of the Emirati Civil Transaction Law stipulates that (The author of any tort, even if not discerning, shall be bound to repair the prejudice) and article no 292 of the same Law stipulates the following:(Damages shall, under all circumstances, be assessed to cover the prejudice sustained and the lost profit provided it is a natural consequence of the prejudicial act.). Through the extrapolation of these texts together, we find that the source focus of compensation for the prejudicial act incurred by others is the law and in order to enable the third party to claim for compensation law necessitates the availability tort liability bedrocks[14]) namely:

First – Fault

According to UAE the fault is built on infringement which means that the person who deviated from the usual behavior, and in our case, the fault that the legislator assumed is committed by the authentication services provider represented in issuing incorrect and defective authenticated certificate which led to damage incurred by others.

Second – Damage:

Damage is presumed by law as soon as a fault occurred by the provider as the law assumed that the third party had suffered from damage as a result of the provider's issuance of an incorrect or defective certificate, and the damage that requires compensation here is the damage actually in addition to the expected damage in accordance with Article 292 of the Emirati Civil Transactions Law which stipulates that aggrieved party can claim for compensations from the provider against the damage that actually occurred as well as the lost profit.

Third – Causal Relationship

Damage that is incurred by others as a result of authentication services provider's fault and the causal relationship the presumed legally if the aggrieved proved the occurrence of the fault and damage can be the debtor (provider) of the authentication services shall and defend and negate the causal relationship between the fault and the damage if the authentication services provider proves that the fault occurred as a result of a reason beyond it reasonable control, which we will discuss later[15].

Third: Cases of Authentication Services Provider's Non-Liability

Article no. 21/5 of the Emirati Electronic Transaction & Commerce Federal Law stipulates that (the authentication services provider shall not be liable towards and damages in the following two cases:

1. If the provider included in the electronic authentication certificate a statement which indicates the scope and extent of its liability towards any relevant person in accordance with the regulation of which is published in this regard?
2. If it is proved that the provider didn't commit any fault or negligence or the damage occurred by an outside reason which is beyond its control.

Article no. 2 of the Emirati Civil Transactions Law stipulates that (if a person proved that the damage occurred because of an outside reason which exceeds its reasonable control such as flood, lightening, sudden accident, force majeure, act of others or aggrieved person's act then the providers shall not committed to provide insurance unless the law stipulates otherwise). In the first case of the text, the provider can relief itself from the liability for the damage the might incurred by the contractor or to define the amount of insurance in the contract or to limit the scope of the liability in the concluded contract such as the limitation of the certificate validity by a certain period and thus limit its liability with its effective date only and the provider can limit its liability through putting certain limit to the value of the transactions to use the authenticated certificate which permissible in the contractual relationship and mentioned in the general rules of the Civil Transactions Law[16].

[14] Dr. Tamer Al-Demyati – previous resource, page 511.
[15] See Dr. Abdul Razzaq Sanhori - the Mediator in Explain the Provisions of the Civil Law, Part No. One – Dr. Monthir Al-Fadel - The Mediator In Explaining Civil Law - Sources of Commitment and Conditions - Comparative Study, p. 252 et seq.
[16] Dr. Tamer Al-Demyati – previous resource, p. 518 as well as the direction issued by the European Parliament on 13/12/1999 concerning the e-signature- article no. 6 thereof.

The parties of the contract may agree on the amount of compensation in the event of a breach by the provider of the contract in executing of the contract or to absolve itself from responsibility, as is well known that the contract is subject to the will of the contractors alone and as long as the parties agreed to determine the scope of the contractual liability or exemption thereof, it is permissible and subject to their authorities and capacities[17].

With regard to tort liability mentioned in the second paragraph of article 21/5 and in accordance with the provisions of Article 296 of the UAE Civil Transactions Law any clause exempts which from tort liability is null and void (Any condition exonerating from tort liability shall be deemed null and void)[18]. By referring back to the test of article no. 21/5/2 of the Emirati Electronic Transaction & Commerce Federal Law and article no. (287) of the Emirati Civil Transactions Law the authentication services provider can negate it responsibility towards compensation and guarantee if it proved the damage occurred and incurred by others for reason beyond its reasonable control if such damage happened as a result of other's act or for reasons attributed to the aggrieved itself or due to force majeure, sudden incident or for any other reasons that are beyond its control or scope.
If the authentication services provider proved that it has no relation with the fault and is out of its control and will then it shall not be responsible for providing guarantee to others[19].

Conclusion and Recommendations

After reviewing the definition of the electronic authentication services providers and how to get the license and the tasks entrusted to the provider and the requirements imposed by law and regulation, and after addressing mistakes that provider might commit during the implementation of the authentication services, as well as the legal texts that deal such faults and compensation both for the party to the contract with the provider or third parties affected by fault. It was noticed such faults and mistakes were treated by the Emirati legislator in the Electronic Transaction & Commerce Federal Law and Civil Transactions Law Case that the electronic authentication service provider could disclaim responsibility was also explained. It was also show that the provider can determine the scope of this responsibility in the contract, both in terms of time and place or quality and it could also determine in advance its amount in the contract it could include a condition through which it could exempt itself from assuming such responsibility. The provider can also disclaim its responsibility to be assumed by the unaffected party in case specified by the Emirati legislature in the general rules of both the Electronic Transaction & Commerce Federal Law and Civil Transactions Law. In such cases, the fault, mistake or defect occurs due to external and outside reason which transcended its control and will or as a result of a force majeure, or because the aggrieved person's own acts.

It worth-mentioning to refer a very crucial point that the provider my require within the framework of the contractual relationship to exempt itself from responsibility, which is very important especially when the provider is a foreigner and deal is made between spaced parties and it is possible they do not know each other or that some of them does not have sufficient knowledge in the field of e-commerce and digital signatures.

I recommend in my modest study the Emirati legislator to the importance of paying more attention to this problem in times or regulations and legislations, especially such services are new to our societies and usually the provider has enough experience and good knowledge more than the contractor. Therefore I recommend to the Emirati legislator to review licensing conditions and terms or the regulation so that more attention shall be given to the contracting party since few number of companies monopolize such contracts, therefore Telecommunications Regulatory Authority has to require the provider of the electronic authentication services to review the conditions and terms of the contract which it uses in concluding contracts with the public so that more attention shall be paid to the contractor in the terms and conditions of the contract as well as taking into account the extent of the contractor's knowledge and experience compared with the provider in the field of information technology and e-transactions, authentication certificate in terms of its importance and danger with reference to the contractor who might be an investor, merchant or the like.

[17] See Dr. Abdul Razzaq Sanhori - the Mediator in Explain the Provisions of the Civil Law, Part No, page 556 – Dr. Tamer Al-Demyati – previous resource, p. 510
[18] See Judge Ibtesam Al-Badwawi – Head of the Third Civil Department in Dubai Courts. Available on the following website: ***http://www.emaratalyoum.com/***
[19] See Dr. Abdul Razzaq Sanhori - the Mediator in Explain the Provisions of the Civil Law, Part No. One – Dr. Monthir Al-Fadel – previous resource, p. 332 et seq .

Consequently, I call the Emirati legislator to put into account the contractor's interest with in case the provider requires in the conditions and terms of the contract to be exempted from the contractual responsibility towards the contractor in case of the occurrence a fault, defect, error or non-compliance with laws and regulations.

References

A. Books & journals

1- Dia Mchaymech, electronic signature - Study compared, the lawful and publications issued in 2003
2- Dr Abdul Razzaq Sanhouri , the mediator to explain the provisions of the civil law.
3- Dr. Tamer Damietta, proving electronic contracting online Study compared to 2009.
4- Nawafleh, et al, E-Government Between Developed and Developing Countries, Journal IJAC, Volume(5), Issue(1), Page 8-13, 2012.
5- Dr. Munther Alfadel. aloset to explain civil law , sources and terms of commitment , a comparative study
6- lawyer Omar Momani , electronic signature and the law of e-commerce, Dar Wael for publication in 2003

B. Legislation

1- UAE Civil Transactions Act
2- Transactions Act and electronic commerce UAE.
3- Regulations for the Law -commerce transaction UAE No. 1 of 2008.
4- Jordanian civil law

C. Electronic sites

1- Lawyer Neven Kstas, responsible for the civil providers of certification services according to Syrian law , available on the website www.syrianbar.org.
2- Judge Ibtisam Alibdwaoa, the exemption from the requirement of civil liability, is available on the website www.emaralyoum.com.