The Legal Framework for Electronic Signature in Jordan
A Comparative Study with EU Regulations

AL ANIMAT, MOHAMMAD ELAYAN KARIM*

ABSTRACT *Electronic signature, owned by the owner is a matter of trust, and it may be difficult for the other contracting party to verify its authenticity , hence the importance of dealing with and organizing digital signature is of paramount importance., The aim of this study is to compare the legislation of the EU and Jordan in governing the responsibility of the authentication service provider concerning electronic signature, to find out whether there is a lack of organized legislation with regard to the work of electronic signature service providers. The article will also examine the adequacy of general regulations in supervising the duties of electronic service providers under Jordanian law. I will emphasize the importance of establishing specific regulations, and the need to establish special rules for this particular responsibility, especially with regard to the development of specific rules in line with the UNCITRAL model law on electronic signatures. As regards the EU directives on electronic signatures and other international legislations, it must be emphasized that the issue of electronic authentication services raises several legal problems that can be resolved. Among others the legal nature of the liability of electronic authentication service providers, their legal basis, and their establishment are still subject to legal controversy. In addition to the scope of this responsibility and the issue of determining the extent of compensation that can be imposed in the event of harm to the customer or others, the Jordanian legislators have not established a specific legal system for the responsibility of the employer and the electronic authentication provider to clarify all the ambiguities to which electronic banking operations are exposed to in order to create an independent and sustainable legislative environment for all the rapid technological development.*

KEYWORDS *electronic bank, security, digital, certificate, authentication*

1. Introduction

Countries are increasingly interested in preparing and issuing legislation that ensures the creation of the legal infrastructure for e-commerce and also the removal of obstacles to its prosperity in a manner that ensures the enhancement

* PhD student, University of Debrecen, Marton Géza Doctoral School of Legal Studies.

of confidence in transactions that take place over the internet. The aim is to provide safe methods for verifying the identity of the contractors, as well as ensuring the security of information transmission in a virtual world surrounded by a set of considerations related to the security and safety of electronic transactions. The need to provide the greatest degree of confidence in these transactions arose, which is represented mainly by the need to verify the validity of these contracts and their issuance by whom they are attributed. For this reason, written and electronic signature have emerged as tools that are consistent with the nature of electronic transactions. Electronic signature has formed one of the most prominent components of electronic commerce and many forms of this signature have emerged, such as the electronic pen signature and biometric signature.[1] Nevertheless, resort to signature goes beyond the problems that would have been caused by the use of ordinary written ones. The electronic one raises the issue of confidence in the attribution of the signature to its owner, and thus in the electronic transaction in general, as it may be difficult for the other contracting party to verify the authenticity of this signature and to attribute it to its owner. This highlights the need for a neutral and trusted party to be the link between the sender and the addressee within this field. Hence the importance of dealing with digital signature and with the existence of a system[2] is to verify the authenticity of digital signature and attribute it to its owner. Electronic authentication is the system in which an electronic authentication service provider issues an electronic certificate that includes elements and data specified by the law that ensures the validity of digital signature and guarantees its attribution to its owner. Through this the authentication authority verifies the integrity and validity of the data contained in the certificate in a manner that gives third parties confidence in the integrity of the transaction that he submits.
This task was undertaken by the electronic authentication service providers, who play the role of mediator between the parties and are subject to a special legal system. Their provisions are regulated by special rules expressed in the law on electronic transactions in countries such as Britain and France. Nevertheless, the Jordanian Electronic Transactions law does not explain in a clear, precise and detailed way how an electronic certificate should be granted.

[1] For a review of the concept and effects of a digital signature and a certificate of authenticity, see Aiman Musaed, "Digital Signature and Certificate of Authenticity: Concept and Legal Implications," *Al-Manara Journal – Al al-Bayt University* 11, no. 4 (2004): 12., and see also online for more information Lorna Brazell, *Electronic Signatures – Law and Regulation* (London: Sweet and Maxwell, 2004), 66–58., and Paul R. Rice, *Law: Electronic Evidence Development and Evidence* (American Bar Association Publication, 2008), 11.

[2] Lina Ibrahim Youssef Hassan, *Electronic Documentation and the Responsibility of the Competent Authorities* (Amman: Dar Al Raya, 2009), 101.; Al-Jammal Saud, *Contracting Through Modern Communication Techniques* (Cairo: Dar Al-Nahda Al-Arabiya, 2006), 321.; Al-Sabaheen Sami, "Electronic Signature And Its Authority In Proof" (PhD diss., Amman Arab University, 2005), 156.; Maître Bernard Burn, *Nature Et Impacts Juridiques De La Certification Dans Le Commerce Électronique Sur Internet*, Mars 2000, https://www.lex-electronica.org/files/sites/103/7-1_brun.pdf.

This is the justification and the importance of this study, as it will make an attempt to shed light on the shortcomings contained in the Jordanian electronic transactions law. It will also try to find appropriate solutions to this problem, by using the provisions of comparative legislation that had previously organized the topic accurately. The complexity involved in proving the traditional conditions of liability prompted the legislators of many states to regulate them with special provisions. Since this issue has not been written about yet, I will intend to demonstrate the present situation. This topic, namely the the development concerning legislation has not been discussed in Jordan yet, and this is one of the difficulties and challenges that I faced. That is the reason why I relied on the comparison with international legislation, analyzing it, and obtaining a clear picture of the subsequent needs. The EU legislators were alerted to the need to intervene in the regulation of the electronic authentication process and the responsibility resulting from it, given the role this process plays in facilitating and flourishing electronic commerce.[3] Thereafter, French legislators harmonized their law with the EU directive, and regulated the process with Trust law,[4] which established a special responsibility for electronic authentication service providers within the official economy for the year 2004, inspired by the provisions of the EU directive.

The importance of this study emerged from an attempt to demonstrate the adequacy of the general provisions on liability to cover the liability cases of the electronic authentication provider, and to examine whether there is a need for the Jordanian legislators to adopt rules for the liability of electronic authentication service providers.

2. Methodology and data used

This article is built on the comparative-analytical approach that aims to facilitate access to facts. The aim is to analyze the principles of digital signature related to the topic of research, by discussing the methods currently used in electronic financial operations. I will present some examples of judicial rulings of the EU Court of Justice and recommendations of the EU directive in this regard. I will also deal with the regulations and instructions of the Jordanian Transaction law concerning the principles of electronic digital signature and methods of cyber adaptation and will draw some important conclusions as regards the UNCITRAL model law on electronic commerce and related laws issued by the Untied Nations.

In this article, the definition of the scope of responsibility and the issue of determining the extent of compensation that can be imposed in the event of

[3] Éric A. Caprioli, "La directive européenne 1999/93/, du 13 décembre 1999, sur un cadre communautaire pour les signature électronique," https://www.caprioli-avocats.com/ .

[4] Philippe Le Tourneau*, Contrats informatiques et électroniques* (2006), 11.; *Droit de la responsabilité et des contrats; Neveux les prestataires de service de certification*: *quelle responsabilité pour quelle service* (2022), 39.

damages to the customer or to third parties appear, since the Jordanian legislators have not set a specific legal system for the responsibility of the third party.The importance of this study emerged from an attempt to prove the adequacy of the general provisions of liability to cover liability issues for the electronic authentication provider, and to reveal whether there is a need for the Jordanian legislators to adopt rules for the liability of electronic authentication service providers.

3. The legal framework for the responsibility of the electronic documentation service provider

The Jordanian legislation within the Electronic Transactions law did not address the civil liability of documentation service providers, because the Jordanian legislator did not regulate the subject with special provisions.[5] The regulations were limited to electronic systems and imposed financial penalties and fines for providing false data. As a result, it was necessary to resort to general rules to determine the legal liability of the electronic documentation service provider.
However, the EU legislation affected by the EU directive on electronic signatures has adopted a system of responsibility for electronic authentication providers,[6] and this prompts us to study the most important features of this system in an attempt to push the Jordanian legislators to consider the legislation and follow the approach in developing special provisions to regulate the legal liability of authentication service providers in Jordan. It also raises the question of the nature of the responsibility arising from the electronic authentication process and its legal basis. Whether it should be included within the framework of contractual responsibility based on the provider's breach of the electronic authentication contract that binds the customer who obtained the certificate or it should be included within the scope of the default nature of the responsibility based on the provider's breach of the imposed legal obligations, according to the legislation that regulated the electronic authentication process. Therefore, concerning the legal nature of the liability of the electronic documentation service provider, it can be said that the specificity of the electronic authentication process and the complexity of the relationships resulting from the issuance of the electronic certificate justify the possibility of envisioning several assumptions of responsibility arising from electronic authentication services. Consequently, the contractual liability of the responsible party of the provider towards the certificate holder and the hypothetical responsibility of the provider towards others can be imagined.[7]

[5] Article 25, Electronic Transactions Law No. 15 of 2015.
[6] Directive 93/13/EEC protects consumers in the EU from unfair terms and is amended by Directive (EU) 2019/2161.
[7] Adnan Ibrahim Al-Sarhan, and Nouri Hamad Khater, *Explanation of Civil Law. Sources of Personal Rights* (Amman, 2021), 302.

There is a relationship between the provider of electronic authentication services and the holder of the certificate regulated by the electronic authentication contract. There is also a relationship between the provider and third parties who rely on the electronic authentication certificate to conclude some actions.[8] There is a relationship between the holder of the certificate and others, which is based on a contract that they wish to conclude, and which is the subject to the provision on specific goods or services.[9] This raises the question of responsibility arising from all of the damages resulting from a defect in the electronic documentation process. Whether the provider is responsible, whether it is the liability of the client holding the certificate, whether it is possible to envisage exempting the provider from liability or liability can be limited.

4. The contractual framework for the service provider

It is understood that contractual liability arises from the occurrence of damage resulting from the debtor's breach of an obligation deriving from the availed contract. This breach is either the debtor's failure to perform his obligations or is due to an existing and valid contract. As a consequence the client who owns the certificate of authenticity may suffer defective implementation or even delay fully or partially. The application of damages as a result of a breach by the authentication service provider is one of his obligations under the authentication contract concluded between them or under the stipulations of the law.[10] Pursuant to this the authentication provider and the client holding the certificate have the right to set what is required if a provider breaches. They may enter into reciprocal terms and obligations according to the principles of contractual freedom and the authority. If the provider of documentation services,[11] or the client, undertake one of these obligations, their contractual responsibility is held.[12] At the same time, contractual liability arises as the electronic authentication contract imposes mutual obligations on both parties, and any breach by the provider or the certificate holder of the obligations incumbent on

[8] Peter Mell, Jim Dray, and James Shook, *Smart Contract Federated Identity Management without Third Party Authentication Services* (Bonn, 2019), 15.

[9] Shu Yun Lim, Pascal Tankam Fotsing, Abdullah Almasri, Omar Musa, Miss Laiha Mat Kiah, Tan Fong Ang, Reza Ismail, "Blockchain Technology the Identity Management and Authentication Service Disruptor: A survey," *International Journal on Advanced Science, Engineering and Information Technology* 8, no. 4-2 (2018): 1735-1745.

[10] For the nature of the contractual relationship between the certification service provider and the signature holder, see Mark Plotkin, *E-Commerce Law and Business, The Nature of the Contractual Relationship between the Certification Service Provider and the Signature Holder* (USA: Aspen, 2003).

[11] Abdel Fattah Hegazy, *Introduction to electronic commerce in Arabic* (Alexandria: University Thought House, 2003), 7.; Caprioli, "Régime juridique du Prestataire," https://www.caprioli-avocats.com/.

[12] Pierre Trudel, France Abran, Karim Benyekhlef, and Sophie Hein, *Droit du cyberespace* (Montréal: Éditions Thémis, 1997), 3.

each of them assesses the party's contractual responsibility. It is often included in contracts that the provider is obligated to confirm the validity of the data contained in the certificate and to verify, if it is attributed to the owner of the electronic signature, even if it is not determined by a special provision of law. This is because the commitment constitutes the core and basis of the electronic documentation process. It is the formula of the agreement the define the nature of the obligation and states whether it is a commitment to reach a result or it is just an obligation to exercise care.[13]

In the absence of a legal provision that establishes this obligation, there is nothing to prevent the parties from including any clause in the electronic authentication contract that stipulates the obligation of the provider to save the personal data of the client who holds the certificate and that it may not be used, processed, or given to others without the client's consent. The provider may be obligated under this condition not to modify, or delete any data related to the customer without the consent of the person concerned. Accordingly, the provider is contractually liable for any breach of the obligation to create, use or trade this data without the consent of the customer. As for the obligation to suspend or cancel the electronic authentication certificate, it was regulated by the Jordanian electronic Transactions law and imposed penalties for breaching it. Nevertheless, if the parties agree on the provider's obligation to suspend or cancel the certificate upon the customer's request, or if there are reasons for its suspension or cancellation, the provider's contractual liability must be based on any damage resulting from the provider's breach of this obligation.[14]

This can be applied to any breach of another obligation contained in the electronic authentication contract, where the provider's contractual liability arises for breach thereof. It is also possible to envisage the supplier's contractual liability towards third parties if the latter was linked to a direct contractual relationship, and the breach of the implementation of this contract resulted in damages.

In a situation where a third-party electronic authentication provider is involved, the certificate that was viewed as a result of a contract he had with them becomes invalid, revoked, or suspended without the authentication services provider informing him. This causes him harm because he had entered into contracts with clients who had the certificate based on the trust he had gained from it, when discussing the provider's and third-party's doctrinal relationship, it's important to consider how the certificate is obtained: directly from the provider or, more practically, from the certificate holder or the authentication provider. However, if the third party obtained the authentication certificate and the public key directly from the certificate holder, we are facing a contractual relationship between the provider and third parties, and therefore it is not possible to imagine the contractual liability of the provider. The third party may also obtain the authentication certificate and the public key from the provider as

[13] Peter Mell, James Dray, and James Shook, *Smart Contract Federated Identity Management Without Third-Party Authentication Services* (Bonn, 2019), 15.

[14] Article 25, Electronic Transactions Law No. 15 of 2015.

a result of a contract,[15] which leads to the possibility of conceiving the existence of a contractual relationship between them, with which the third party was associated with the provider of authentication services and thus the possibility of raising the rules of contractual liability if the third party who relies on this certificate incurs any damages.[16]

This way arises the possibility of conceiving contractual liability for damages incurred by third parties, who also see reliance on the certificate vis-à-vis the provider based on the stipulation theory for the benefit of others. Thus, all damages may be inflicted on third parties because they rely on the electronic authentication certificate. In fact, the contractual liability of the electronic authentication service provider raises several questions that the general provisions may fall short of answering. Some difficulties may arise during implementation, such as the need to prove the error of the electronic authentication provider, nevertheless it is often difficult to prove. The existence of a contractual relationship between the parties must also be the proprietor of the contract to arise. This is difficult to imagine in practice, as there is no contractual relationship between them in most cases.

The multiplicity of relationships arising from it, in addition to the technical and modern nature of the various techniques of electronic signature and authentication certificates, the issue of determining the nature of the provider's commitment and whether it constitutes an obligation to take care or achieve a result; makes the burden of proof difficult[17]. The parties can undoubtedly avoid these difficulties through the terms agreed upon in the electronic authentication contract. Therefore, the parties should be vigilant and careful when drafting the terms of this contract, especially those related to the terms of the exemption and mitigation of liability, since many of these terms may be considered a kind of arbitrary terms that are subject to deletion or modification. In particular, the provisions of EU directive of 5 April 1993 on unfair conditions can be applied to the relationship between customers and suppliers, and directive 93/13/EEC protects consumers in the EU from unfair terms and conditions which might be included in a standard contract for goods and services they purchase. As part of the New Deal for Consumers the notion of 'good faith'[18]is introduces to avoid any significant imbalance in mutual rights and obligations.

The electronic Transactions law of 2001 is devoid of any provision specifying the conditions for cases where the documentation provided is responsible and its legal system is clarified. The legislators are satisfied with including provisions that impose a criminal penalty for issuing an inaccurate, suspended,

[15] Anwar Yaqoub, *Civil Liability of the Certification Service Provider*, 313.

[16] The public key: is the symbol assigned or approved by the electronic authentication authorities to a user Electronic authentication certificate in order to verify the validity of the electronic signature; according article 2, Electronic Transactions Law No. 15 of 2015.

[17] Al-Sarhan, and Khater, *Explanation of Civil Law*, 302.

[18] Directive (EU) 2019/2161, which aims to modernise EU consumer law and improve its enforcement.

or revoked certificate of authenticity. In light of the absence of a special provision it is not possible to establish the liability of the electronic documentation service provider. In the Jordanian legislation it was necessary to resort to the rules concerning civil liability. In order to provide confidence in these transactions the electronic signature has emerged as a tool in line with the nature of electronic transactions. The validity of these contracts must be emphasized because electronic signature is the most important means of electronic commerce.[19]

When taking an extensive look at the legal and financial rules and principles of the UNCITRAL law regarding ratifications of service providers and the most important regulatory reference points, we will address the EU directive in this regard. International use of electronic authentication and signature methods may also benefit from the adoption of UNCITRAL standards, for electronic and paper-based digital signature systems.[20] The criteria for functional equivalence between electronic signatures and paper ones may provide an international common framework for allowing electronic authentication and signature methods to meet foreign signature requirements. Some problems may persist, however, in connection with the international use of such methods that require the involvement of a trusted third party in the authentication or signature process.[21]

5. Place of origin reciprocity and local validation

One of the most important obligations of a local certification service provider, certification authority or regulatory authority is to have country-specific signatures and certificates for some form of verification. Based on reciprocity, signatures and certificates are legally issued by one country to another. Many recognition systems are likely to have some discriminatory effects when not intended; for example, if you are incorporated in a non-EU country, you have three options for certification recognition. If you are in the EU, certification service providers must meet the requirements of the EU electronic signatures directive and will have accreditation under a system set up in a member state.[22] The directive effectively requires foreign certification service providers to comply with both their home country and EU regulations, which is a higher

[19] Electronic Transactions Law No. 85 of 2001.

[20] Trudel, Abran, Benyekhlef, and Hein, *Droit du cyberespace*, 33.

[21] UNCITRAL Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods, (Vienna: United Nations, 2009).

[22] Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/ec article 25/3 legal effects of electronic signatures: a qualified electronic signature based on a qualified certificate issued in one member state shall be recognized as a qualified electronic signature in all other member states.

standard than would be required of certification service providers accredited in a member state. In addition, the EU directive on electronic signatures has been implemented with some deviations. Ireland and Malta, for example, recognize foreign digital signatures (creditable certificates in EU terminology) as equivalent to domestic signatures provided that other legal requirements are met. On the other hand, recognition is subject to local verification (Austria, Luxembourg) or a decision by a local authority (Czech Republic, Estonia, Poland) and this tendency to insist on some form of local verification, usually justified by legitimate concerns, regarding the reliability of foreign certificates. It leads in practice to a system of distinguishing foreign certificates according to their geographical origin. The EU directive on electronic signatures requires foreign certification service providers to comply with both their original data and the EU system, which is a higher standard than the accredited certification service providers in an EU member state.[23]

One of the most important documents was the EU directive on electronic signatures. Article 6 of this directive included a legal regime for the responsibility of the French provider of electronic documentation services in confidence in the digital economy in 2004, to confirm this trend. Authentication services with specific rules by the nature of the tasks performed by these providers and the role they play were given the extreme dominance of the electronic authentication process in internet contracting and commercial trust. The directive includes several rules that highlight the specificity of the rules of liability for services however, electronic documentation is distinguished from the general rules of liability, At the same time the EU directive established the legal system for the liability of suppliers on several grounds, including the obligation to distinguish between an approved electronic certificate and a non-accredited certificate. It also resorted to strictness in the responsibility of the suppliers, as it is an assumed responsibility**,** (the EU directive also allowed the possibility of limiting the extent or scope of his responsibility, unless the provider proves the opposite).[24]

On November 11, 2020, the Court of Justice of the EU held that the near-field communication (NFC) functionality of a bank card, also known as contactless payment, in itself is a "payment instrument" as defined in the EU payment services directive 2015/2366 PSD 2, and the ECJ also clarified the meaning of "anonymous use" under PSD 2 about NFC functionality. The Court stated that a bank may not exclude its liability for unauthorized low-value transactions in its general terms and conditions by simply claiming that blocking the NFC

[23] Article 7, European Union directive on electronic signatures, Article 7, Eligibility for notification of electronic identification schemes An electronic identification scheme shall be eligible for notification pursuant to Article 9 (1).

[24] Valérie Sédallian, and Jérôme Dupré, "Le développement du commerce electronique," *Le contrat d'achat informatique: Aspects juridiques et pratiques* (Vuibert, 2005); Caprioli, "La directive européenne 1999/93/, du 13 décembre 1999, sur un cadre communautaire pour les signature électronique," www.europea.EU.intal/comm/dg/fr.

functionality would be technically impossible but must prove impossibility in light of the objective state of available technical knowledge when a customer reports a lost or stolen bank card. Furthermore, the Court ruled that if the user is a consumer, general terms and conditions provide for tacit consent to possible future amendments to such terms and conditions and must comply with the standard of review set out in directive 93/13 on consumer rights protection, not with PSD2. It defines the responsibilities required from each party and defines the responsibility of the certificate authentication service provider, which defines the actions of the authorized party. The relying party bears the legal consequences of failing to do so; (i) take reasonable steps to verify the authenticity of an electronic signature, (ii) if the electronic signature is supported by a certificate, reasonable steps shall be taken; (iii)verifies that the certificate has been suspended or revoked and that any certificate restrictions are observed.[25]

6. Discussion

The idea seems to be that a party intending to rely on an electronic signature should consider whether and to what extent such reliance is reasonable in light of the circumstances. It is not intended to address the issue of the validity of the electronic signature, which is addressed under article 6, and should not be dependent on the behaviour of the relying party. The question of the validity of an electronic signature should be separated from the question of whether it is reasonable for a relying party to rely on a signature that does not meet the standard set out in article 6.[26] Whereas article 11 may place a burden on authorized parties, particularly when such parties are consumers, it may be recalled that the model law is not intended to invalidate any rule governing consumer protection, nevertheless, it may play a useful role in educating all relevant equal relationships, including authorized parties, regarding the standard of reasonable conduct that must be met concerning electronic signatures. In addition, establishing a standard of behavior whereby a relying party must validate the signature through accessible means may be seen as necessary for development.[27]

The electronic signatures model act of 2011 must be emphasized, which outlines the responsibilities required from each party and delineates the

[25] Jenny Gesley, European Union: European Court of Justice. Rules on Liability of Banks for Unauthorized Low-Value Transactions Using Contactless Payment, *Library of Congress* 2020. https://www.loc.gov/item/global-legal-monitor/2020-12-21/european-union-european-court-of-justice-rules-on-liability-of-banks-for-unauthorized-low-value-transactions-using-contactless-payment/.

[26] Article 6, UNCITRAL Model Law on Electronic Signatures with Guide to Enactment UNITED NATIONS (New York, 2001).

[27] Article 11, UNCITRAL Model Law on Electronic Signatures with Guide to Enactment UNITED NATIONS (New York, 2001).

responsibility of the certificate authentication service provider, and outlines the procedures for the authorized party. The relying party bears the legal consequences for failing to take reasonable steps to verify the authenticity of the electronic signature. Provided that the electronic signature is supported by a certificate, reasonable steps must be taken to verify that the certificate has been suspended or revoked and that any restrictions related to the certificate are observed. Under article 11 a party intending to rely on an electronic signature should consider the question of whether and to what extent such reliance is reasonable in the light of the circumstances. It is not intended to address the issue of the validity of an electronic signature, which is dealt with in article 6 and should not depend on the conduct of the relying party. The validity of an electronic signature should be separated from the question of whether it is reasonable for the relying party to rely on a signature that does not meet the standards set forth in article 6.

While article 11 may place a burden on authorized parties, particularly where such parties are consumers, it may be recalled that the model law is not intended to override any rule governing consumer protection, however, the model law may play a useful role in educating all related equal relations, including authorized parties, and the standard of reasonable conduct that must be met in connection with electronic signatures. In addition, establishing a standard of behaviour according to which the relying party must verify the validity of the signature through accessible means may be seen as essential to the development of any public infrastructure system infrastructure system.[28]

Finally, I believe that reliance on the reasonableness of reliance on the certificate of authenticity, as a condition for the service provider's civil liability is necessary to strike a balance between providing protection to third parties and moving away from imposing excessive obligations on the provider. If it is unreasonable for a third party to rely on a defective authentication certificate because of its previous dealings with the certificate holder or by the nature of the transaction, it is not reasonable to say that the authentication service provider is responsible in this case. The provider’s responsibility for the damages resulting from the electronic document may be negated if one of the reasons for the general rules of liability is present, including force majeure, the act of third parties, and the action of the injured party.

As for the decision according to force majeure as the reason for the supplier’s negation of liability, the supplier’s liability for the damage caused may be nullified if he proves that the damage occured due to an uncontrollable cause and is due to an unexpected event outside his control. There may be exceptional reasons beyond the will of the parties, such as the failure of an external person, however it is required that it is unexpected and that the occurrence and damage of the electronic devices used in the electronic authentication processes are due to the occurrence of an earthquake, volcano, wars or floods.

It is noted that these cases revolve around the non-liability of the provider due to the act of the customer holding the certificate or his decision of the general

[28] Article 11, UNCITRAL Model Law.

rules on liability. Thus, the provider's act is influenced by a third party and is not the consequence of force majeure, and the damage that arised is due to other factors and he is not responsible for suspending or cancelling the stipulations of the certificate.[29]

Similarly, if the certificate holder fails to keep the secret number of the electronic signature confidential or fails to inform the provider if a third party has obtained or taken control of the private key, or if any modifications have been made to the data after the certificate has been issued, the responsibility of the provider may be negated. Additionally, if it can be proven that it is not reasonable for a third party to rely on the electronic authentication certificate, such as in cases where the certificate has been suspended or permanently revoked, and this is clearly indicated in the electronic certificate registry that the provider is required to maintain, this will be considered as a valid reason for the provider not being liable for any damages resulting from unreasonable reliance on the electronic certificate.

7. Conclusion

The study deals with issues that previously have not been touched on. I researched the writings and articles that experts discussed in the past. This topic has not been discussed in Jordan yet, and this is one of the difficulties and challenges that I faced, so I relied on comparison with international legislation, analyzing it, and obtaining a clear picture of the subsequent needs.

Indeed, interested customers may encounter a legal void and instability related to legal liability, the conditions for its creation, and the consequences associated therewith when engaging in electronic signature activities. The Jordanian legislators did not explicitly address these points within a specific, detailed, and comprehensive legal framework of all possible developments in the accelerating world of electronic commerce, which raises questions about liability, including the liability of the provider for damages resulting from defects in the electronic authentication process, and the responsibility of the customer for violating the certificate.

The Jordanian legislators must realize the importance of developing laws, especially those working in the field of information technology and financial transfers as they need to be developed continuously to keep pace with the course of global electronic commerce, avoid legal instability, and use the European experience to be a motive for setting the exact details and required legislation and clarifying any ambiguity, as stability encourages investors in the field of electronic commerce to move forward.

[29] Hegazy, *Electronic Commerce*; Caprioli, "Régime juridique du Prestataire," https://www.caprioli-avocats.com/.

In addition, the provider is obligated to refrain from deleting, adding, or modifying the personal data necessary to provide and maintain the certificate however the possibility of limiting or excluding the provider's liability remains uncertain. Thus, the provider bears contractual liability for any breach of the obligation to generate or use data without the consent of the customer.