THE RESPONSIBILITY OF ELECTRONIC AUTHENTICATION SERVICE PROVIDERS IN JORDAN: AN ANALYTICAL STUDY*

Mohammad Al Animat[1]

This article discusses the development of special rules for the responsibility in electronic authentication service provision, in particular in relation to the United Nations Commission on International Trade Law (hereinafter UNCITRAL) Model Law on Electronic Signatures (2001) and the European Union Directive on Electronic Signatures (1999/93/EC) (hereinafter EU Directive).

Keywords
electronic signature, consumer protection, UNCITRAL, European Union, Jordan

1. Introduction

The legislative role in issuing instructions and regulations on the approval of digital signatures and validity certificates by service providers within the consumer protection chain is currently a popular topic of discussion. Such legislation is thought to ensure safe banking operations on an ongoing basis during an increase in the risk of financial fraud caused by the technological revolution.

At the same time, the use of an electronic signature requires trust that the signature provider has ownership of the signature. It is often difficult for contracting parties to verify the signature's authenticity, indicating the importance of dealing with and regulating digital signatures. Thus, the aim of this study was to compare Jordanian electronic signature authentication legislation with its international counterparts to identify gaps in Jordanian rules regulating the responsibility of electronic signature authentication service providers. Jordanian law may significantly modernize its regulatory framework for electronic transactions by taking lessons from the EU Directive on Electronic Signatures and the UNCITRAL Model Law on Electronic Signatures. By embracing harmonization, legal clarity, cyber security, promotion, and adaptation, Jordan may be able to establish a climate that is favourable for reliable and secure electronic transactions, encouraging economic development and innovation.

2. Discussion

2.1 Fundamental concepts

The terms "*electronic authentication*" and "*electronic signature*" refer to techniques for replicating some or all of the functions of handwritten signatures in an electronic

* DOI 10.21868/PGnG.2023.2.7.
[1] *Mohammad Al Animat,* PhD Candidate, Géza Marton Doctoral School of Legal Studies, University of Debrecen.

environment (UNCITRAL 2009, 13). The primary goal of an electronic signature is to verify a person's desire to concur with the terms of a document or transaction; the electronic signature guarantees the signed document's legitimacy and integrity. The main goal of electronic authentication is to confirm the identification of a person or system when they visit a digital platform or engage in online activities; it is used to guard sensitive data and stop illegal access. Both electronic authentication and electronic signature are crucial to ensuring the reliability and security of electronic interactions and online transactions. In electronic authentication, the term "*authorizing party*" designates the person or organization with the power of attorney, or "*authorization*", to issue and utilize electronic signatures. This person generally begins the digital transaction by, electronically signing a paper. The party whose intent is being conveyed by the electronic signature is the authorizing party. In other words, they are the signer who applies their electronic signature to show that they concur with, approve of, or assent to a transaction's terms.

The "*relying party*" is any person, group, or other entity that believes an electronic signature is genuine and legitimate. This party depends on the electronic signature to prove that the person who authorized the transaction actually intended to sign the document or conduct the transaction. To be sure that the document was not changed after being signed and that the signer's identity is real, the relying party may need to confirm the signature's legitimacy. The "*dependent party*" in this situation is anyone with an interest in the transaction or agreement that was signed. This includes parties with contractual relationships with the authorized party and other parties that might be impacted by the signed document's content but do not have a contractual relationship.

Electronic signature security and validity are ensured by a certification service provider CSP. Through a procedure known as digital certificate issuing, a reliable CSP aids in establishing the connection between the electronic signature, the party approving it, and the content of the document. The CSP issues this digital certificate, which serves as an authenticity seal, after confirming the identity of the authorized person. By offering another level of validation to the electronic signatures and transactions facilitated by the parties concerned, government recognition and authorization of a CSP or relevant website can increase confidence and security. This certification frequently rests on adherence to particular criteria and guidelines established by the government that guarantee the integrity of electronic transactions.

2.2 Comparative assessment

In fact, non-compliance with the requirements of Article 11 of the UNCITRAL Model Law (UNCITRAL 2002) means a breach of a general obligation, on the relying authorized party to verify the electronic signature or certificate. A question arises when the relying party does not comply with the requirements of Article 11. Not complying with the required data should not prevent the relying party from making use of the signature or certificate if reasonable verification does not reveal the signature or certificate to be invalid.[2] Under the requirements of Article 11, such a case may need to be dealt with by applicable law outside the UNCITRAL Model Law.

[2] „Conduct of the relying party a relying party shall bear the legal consequences of its failure:

While preparing the UNCITRAL Model Law, it was suggested that a distinction should be made between the legal regime applicable to the signatory and the certification service provider (who both face obligations with respect to their conduct inconsistent with the electronic signature process) and the regime applicable to the authorized party (for whom the UNCITRAL Model Law may apply but who do not face the same level of obligation as the other two parties). However, the prevailing view was that the question of establishing such a distinction should be left to applicable law**,** that reliance on the reasonableness of reliance on the Certificate of Authenticity, as a condition of 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 (Kamil, 2008).

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, then it is not reasonable to say that the authentication service provider is responsible in this case. "*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*" (UNCITRAL 2009, Article 6.). The provider's responsibility for the damages resulting from the electronic document may be negated if there is one of the reasons for the general rules of liability, including force majeure, the act of third parties, and the action of the injured party (Lim et al. 2018).

As for the decision according to force majeure as the reason for the supplier's negation of liability, the supplier's responsibility for the damage caused may be nullified if he proves that the damage had to occur due to an uncontrollable cause and is due to an unexpected event outside his control. The reason is exceptional beyond the will of the parties, it is required that it be unexpected and that the occurrence and damage of the electronic devices used in the electronic authentication processes 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 on the general rules on liability. Thus, the provider finds itself liable due to the act of a third party and not because of force majeure, which concerns the damage that arises to others despite the provider suspending or cancelling the functioning of the certificate (Hjazi & Kamil 2015). The responsibility of the provider shall likewise be negated in the case of the certificate holder himself neglecting to keep the secret of his electronic signature from third parties, or failing to inform the provider that a third party was able to obtain or control the private key or that he revealed the secret number for any reason, so that the provider could take the necessary precautions, or not informing the provider of any modification or change to this data after issuing the certificate. If it can be proven that it was not reasonable for a third party to rely on the electronic authentication certificate, due to it having been suspended or permanently revoked – especially if this is clear and indicated in the register of electronic certificates that the provider is obliged to submit –

(a) To take reasonable steps to verify the reliability of an electronic signature; or
(b) Where an electronic signature is supported by a certificate, to take reasonable steps:
(i) To verify the validity, suspension or revocation of the certificate;
(ii) To observe any limitation with respect to the certificate."(UNCITRAL 2002, Article 11.).

proof of this record shall be a reason for unreasonable reliance on the electronic certificate, and therefore a reason for the provider not being liable (Gyorffy et al. 2011).

Article (8) of the European Directive on Electronic Signatures (1999/93/EC) is titled "*Liability*". This article aims to establish the liability of electronic signature service providers for the services they provide: accordingly, electronic signature service providers are liable for any damages caused by their service, either to the signatory or to any third party. This includes any damages caused by errors, omissions, or negligence in the provision of electronic signature services, and the liability of the service provider is limited if the damage was caused by circumstances beyond their control, or if the damage was caused by an act or omission of the signatory. Article (8) also requires member states to establish procedures for the investigation and resolution of disputes related to electronic signature services. These procedures should be accessible, simple, and inexpensive, and the European Directive on electronic signatures establishes the liability of electronic signature services providers and provides a framework for the investigation and resolution of disputes related to electronic signature services (EU Directive).

However, the European judiciary affected by the European Directive on electronic signatures has adopted a liability regime for electronic certification providers, and the European Union Directive on Electronic Signatures actually requires foreign certification service providers to comply with both their original data and the European Union system, which is a higher standard than certification service providers accredited in a member state of the European Union (Fritz 2020).

Article (8) of the Jordanian Electronic Transactions Law No (85) of 2001, and its amendments stipulate that providers of authentication services and electronic service providers are obligated to take the necessary measures to maintain the reliability and legitimacy of electronic transactions, through the use of electronic signatures, digital certificates, encryption, and electronic documentation of transactions, in accordance with the controls and the conditions specified by the executive regulations of the law.[3] This law aims to promote the safe and reliable use of electronic technologies in commercial and legal transactions, and to encourage investments in electronic commerce in Jordan. The law also guarantees the equality of electronic transactions with paper transactions with regard to law and evidence and protects the rights of consumers and contracting parties in electronic transactions.[4]

Through this article, it is important to emphasize the need to find special texts in the Jordanian legislation that regulate the work of the documentation authorities and the civil liability resulting from the failure of these authorities to perform their work. There are general provisions, however the liability in the Jordanian Civil Code or in the Electronic Transactions Law is not sufficient to provide effective protection for those affected by the electronic documentation process. These texts may not help in determining when to establish the responsibility of providers of electronic

[3] Article (8) of the Jordanian Electronic Transactions Law No. (85) in 2001.

[4] Article (34) of the Jordanian Electronic Transactions Law states the following: The documentation showing the identification code is approved in the following cases: A- It is issued by an authorized party or accredited. B- Issued by an authority licensed by a competent authority in another country and recognized. C- Issued by a government department, institution or body authorized by law. d- Issued by an approved authority the parties to the transaction for approval.

authentication services, as the Jordanian law did not indicate how the authentication process is practiced and the obligations arising therefrom. There is a deficiency in the Jordanian legislation in many aspects of the electronic authentication process, such as what is meant by the process of authenticating the electronic signature, what essential data is to be available in that certificate and the responsibility resulting from it, and some of the obligations on the shoulders of the provider ahead of activating electronic transactions. This has led to a legal vacuum, the intensity of which has further increased due to the failure to put in place the necessary regulations and instructions for practicing the electronic authentication process (Abu-Jassar et al. 2022).[5]

Since most of the obligations of the electronic authentication entity are related more to exerting due diligence than to achieving any given result, we can see that the requirement to prove that the harm to the third party relying on the authentication certificate was due to the negligence of the authentication authority constitutes a practical obstacle to the establishment of legal liability. The technical nature of some of the obligations of the electronic authentication entity is such that others may not be aware of them, which creates a difficulty of proof. To this end, it can be said that it is necessary to assume the error of the authentication authority, which leads to shifting the burden of proof to the authentication authority to prove that it has not breached any of its legal obligations. However, we also see the necessity of not imposing legal responsibility on the documentation authorities, if it is unreasonable for others to rely on the Certificate of Authenticity.

3. Conclusion

The Jordanian legislator must prepare the legal framework accurately and with clear texts to create an investment environment in Jordan for people, as they may find themselves facing instability concerning the legal nature of responsibility, the conditions for its establishment and the consequences thereof. In fact, the Jordanian legislator did not mention these points in a specific legal framework, which raises the issue of the provider's responsibility for all such damages resulting from a defect in the electronic authentication process and for the perception of the customer's responsibility for violating the certificate. He did not say whether it was possible to imagine excluding or limiting the provider's liability.

Under the contract terms, the liability for a data breach lies with the provider, who is responsible for any violations of the prohibition against collecting or using data without the customer's permission. This implies that the provider may be liable for any negative effects or legal problems that result from the use or generation of data without getting the required costumer's authorisation.

Conversely, article 8 of the European Directive on Electronic Signatures puts a responsibility on the provider to keep personal data required for the transmission and maintenance of the certificate from being deleted, added to or modified. This implies

[5] The paper describes a method for ensuring secure electronic authentication of users accessing human-machine interfaces (HMI) or supervisory control and data acquisition (SCADA) systems over insecure Internet networks HMI/SCADA systems are commonly used in industrial environments to monitor and control complex processes, and their security is a source Serious concern given the potential consequences of unauthorized access or malicious attacks.

that the provider cannot change or erase personal data without a valid reason if the data are necessary for the correct operation, delivery or maintenance of an electronic certificate. The article concluded the most prominent was the insufficiency of the general rules to regulate this responsibility, which requires the Jordanian legislator to enact the necessary legal texts to determine the obligations of the authentication service provider and the legal nature of his responsibility while achieving legal balance by requiring reasonable reliance on the electronic authentication certificate.

Finally, comparing Jordanian legislation to the model legislation of the UNCITRAL and the Directive on Electronic Signature of the European Union offers important insights for the improvement of the legal frameworks for electronic transactions and signatures in Jordan. The value of harmonisation and compliance with international standards is one important lesson; the UNCITRAL Model Law and the EU Directive both stress the importance of legal frameworks keeping up with modern technological developments. To guarantee consistency with international standards and ease cross-border electronic transactions, Jordanian legislation should work to embrace comparable concepts.

The comparative study also emphasises the value of legal certainty and clarity. The UNCITRAL Model Law provides a thorough and coherent framework covering many facets of electronic transactions and signatures. Strong cybersecurity measures are critical, as evidenced by the EU Directive's focus on security and authentication systems. To ensure the integrity and confidentiality of electronic transactions and to promote trust among stakeholders, Jordanian legislation should prioritise the implementation of robust authentication procedures and data protection provisions.

In addition, the success of the European Union in enabling the legal acceptance of electronic signatures and encouraging their use highlights the value of aggressive promotion and awareness initiatives. The Jordanian authorities may wish to consider implementing educational programmes to increase business and public understanding of the benefits and legitimacy of electronic signatures and to promote their widespread use. The flexibility of the UNCITRAL Model Law and the EU Directive supports the ability of legal systems to adapt to changing technological environments. In order to accommodate future advances in electronic commerce and electronic signatures without the need for frequent legislative amendments, Jordanian legislation should be drafted with a forward-looking perspective.

References

- Abu-Jassar, A. T. et al. (2022). *Electronic User Authentication Key for Access to HMI/SCADA via Unsecured Internet Networks*, Computational Intelligence and Neuroscience. https://www.hindawi.com/journals/cin/2022/5866922/ [accessed December 2, 2022]
- Caprioli, E. A. (2007). La dématérialisation des documents et des échanges (écrits et signatures électroniques). *Caprioli & Associés. Société d'Avocats.* May 2007, https://www.caprioli-avocats.com/fr/informations/la-dematerialisation-des-documents-et-des-echanges-ecrits-et-signatures-electroniques-21-57-0.html [accessed January 2, 2023]

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. OJ L 13, 19.1.2000, p. 12–20.
- Fritz, V. (2020). European Union: European Court of Justice Rules on Liability Of Banks For Unauthorized Low-Value Transactions Using Contactless Payment. *Library of Congress.* December 21, 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 [accessed January 2, 2023]
- Gyorffy, J. C. et al. (2011). 'Token-based Graphical Password Authentication'. *International Journal of Information Security*, 10: 321–336.
- Hjazi, W. & Kamil, T. (2015). Electronic Signatures, Authentication Service Providers.
- Ibrahim, A. (2018). Documenting Electronic Transactions, Nature et impact juridique.
- Jordanian Electronic Transactions Law No. (85) in 2001. https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/jo/jo058en.html [accessed December 2, 2022]
- Kamil, T. (2008). Electronic Authentication Service Providers (Legal Regulation, Their Duties and Responsibilities). *University of Sharjah Journal of Islamic and Legal Sciences* 5.
- Lim, S. Y. et al. (2018). Blockchain technology the identity management and authentication service disruptor: A survey. *International Journal on Advanced Science, Engineering and Information Technology* 8(4-2): 1735–1745.
- Mell, P. et al. (2019). Smart Contract Federated Identity Management without Third Party Authentication Services, *Open Identity Summit*, March 28, 2019.
- UNCITRAL (2002). Model Law on Electronic Signatures with Guide to Enactment 2001. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf [accessed December 2, 2022]
- UNCITRAL (2009). Promoting confidence in electronic commerce; part one legal issues on international use of electronic authentication and signature methods. https://digitallibrary.un.org/record/657519 [accessed December 2, 2022]