



RESEARCH ARTICLE

Section: *Legal Studies*

Civil liability of electronic signature service providers in light of comparative legislation

Mohammad Mahmoud Said Al Dawoud^{1*}, Yusuf Ahmad Mofleh¹, Eman Al-Wreikat², Suheir Salah Almaaitah¹, Amani Aldabbas³ & Rakan Nayef M. Al Sbeihi⁴

¹Faculty of Law, Zarqa University, Jordan

²Private Law Department, Faculty of Law, Al-Ahliyya Amman University, Jordan

³Lawyer and Legal Consultant, Jordan

⁴Legal Researcher and Jordanian Lawyer, Jordan

*Correspondence: maldawoud@zu.edu.jo

ABSTRACT

The rapid expansion in the use of electronic signatures is accompanied by the emergence of legal challenges relating to the determination of the civil liability of electronic signature service providers, particularly in view of the pivotal role performed by them in issuing authentication certificates, verifying the identity of transacting parties, and ensuring the integrity of electronic transactions. Against this background, the study is aimed at analyzing the civil liability of electronic signature service providers by identifying their legal status, analyzing the legal and technical obligations imposed upon them, and clarifying the legal basis of civil liability arising from breaches of such obligations, in addition to examining cases in which liability is excluded and the conditions governing exemption therefrom, in light of a comparison with Egyptian legislation and European regulation. The descriptive, analytical, and comparative approaches are adopted in the study through the analysis of the legal provisions governing electronic signature services and their comparison with comparative legislative trends. It is concluded in the study that electronic signature service providers constitute one of the most important elements in building trust in electronic transactions and that their civil liability is linked to breaches of the legal and technical obligations relating to identity verification, the issuance of authentication certificates, the management of signature keys, the preservation of data confidentiality, and the management of the certificate life cycle. It is also demonstrated that the liability of the service provider may be contractual or tortious, depending on the nature of the legal relationship, and that most of its fundamental obligations are closer to obligations to achieve a specific result than to obligations to exercise due care, thereby justifying the application of a stricter standard of liability commensurate with the professional and technical nature of this activity. It is further shown that Jordanian regulation, despite providing a legal framework for regulating electronic signature services, still requires greater detail in defining technical obligations, the standard of civil liability, and the conditions governing exemption therefrom, in a manner that enhances trust in the digital environment and keeps pace with rapid technological developments.

KEYWORDS: civil liability, electronic signature, electronic signature service providers, electronic authentication certificates

Research Journal in Advanced Humanities

Volume 7, Issue 4, 2026

ISSN: 2708-5945 (Print)

ISSN: 2708-5953 (Online)

ARTICLE HISTORY

Submitted: 21 June 2026

Accepted: 11 July 2026

Published: 01 October 2026

HOW TO CITE

Al Dawoud, M. M. S., Mofleh, Y. A., Al-Wreikat, E., Almaaitah, S. S., Aldabbas, A., & Al Sbeihi, R. N. M. (2026). Civil liability of electronic signature service providers in light of comparative legislation. *Research Journal in Advanced Humanities*, 7(4). <https://doi.org/10.58256/2tqyxr55>



Published in Nairobi, Kenya by Royallite Global, an imprint of Royallite Publishers Limited

© 2026 The Author(s). This is an open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1 Introduction

In recent decades, the world has witnessed an accelerating shift toward digitalization across various spheres of economic, commercial, and administrative life, resulting in an unprecedented expansion in the use of electronic means for concluding legal transactions and conducting transactions remotely. This transformation has posed new legal challenges relating to the proof of electronic transactions and the assurance of their integrity and reliability, thereby necessitating the development of legal and technical mechanisms capable of providing a level of trust equivalent to that afforded by traditional means of proof (Tawakkul, 2010). In this context, the electronic signature has emerged as one of the most important legal mechanisms for verifying the identity of transacting parties, ensuring data integrity, and conferring legal evidentiary value upon electronic documents, making it one of the fundamental pillars of the digital economy and modern electronic transactions (United Nations, 2001).

The effectiveness of an electronic signature is not achieved merely through the use of the technical means necessary for its creation; rather, it is closely linked to the existence of specialized entities responsible for issuing electronic authentication certificates and managing the associated technical infrastructure (Alsalmi et al., 2026). These entities are known as electronic signature service providers or trust service providers. Such entities perform a fundamental role in enhancing trust in the digital environment by verifying the identity of certificate applicants, issuing authentication certificates, managing electronic signature keys, maintaining data confidentiality, and taking the necessary measures to suspend or revoke certificates when the conditions governing their validity cease to exist. Consequently, the integrity and stability of electronic transactions are largely dependent upon the extent to which these entities comply with the legal, technical, and security obligations imposed upon them (Hijazi, 2007).

The significance of this role is further heightened by the fact that any breach of these obligations may result in legal and financial damage to the holder of the authentication certificate or to third parties relying upon it, whether as a result of issuing a certificate on the basis of inaccurate information, failure to verify the identity of the applicant, breach of data confidentiality, delay in suspending or revoking the certificate, or other forms of breach that may undermine trust in electronic transactions (Alatawi, 2025). This raises legal questions concerning the nature of the civil liability of electronic signature service providers, the legal basis upon which such liability is founded, its limits, and the extent to which the general rules of civil liability are sufficient to accommodate the technical particularities of this activity (Haj Ali, 2013).

Although the Jordanian legislature has regulated electronic signatures through the Electronic Transactions Law No. (15) of 2015 and the regulations issued pursuant thereto, it has not established a detailed framework governing the civil liability of electronic signature service providers commensurate with the nature of the role performed by them in the digital environment, particularly with regard to defining the scope of their obligations, the standard of professional fault, the limits of liability toward contracting parties and third parties, and the circumstances in which liability is excluded or exemption therefrom is permitted (Hashemite Kingdom of Jordan, 2015). By contrast, the European regulation governing trust services (eIDAS) has adopted a more detailed legal framework regulating the obligations and liability of trust service providers, thereby enhancing trust in electronic transactions and providing greater legal protection for transacting parties (European Union, 1999).

1.1 Research Problem

The increasing expansion in the use of electronic signatures has heightened the importance of the role performed by electronic signature service providers in ensuring the reliability of digital transactions, making the determination of their civil liability a legal issue of considerable importance. However, although Jordanian legislation regulates electronic signatures pursuant to the Electronic Transactions Law No. (15) of 2015 and the regulations issued thereunder, it has not addressed the civil liability of electronic signature service providers through a detailed regulatory framework that keeps pace with the technical nature of this activity, particularly with regard to determining the nature of their obligations, the legal basis of their liability, the limits of such liability toward both beneficiaries and third parties, and the circumstances in which liability is excluded or exemption therefrom is permitted (Haj Ali, 2013; Hashemite Kingdom of Jordan, 2015). The significance of this issue is further heightened by the expanding reliance on electronic signatures in digital transactions and by the

consequences that may result from breaches of the legal and technical obligations of service providers, affecting trust in the digital environment and the protection of transacting parties. Accordingly, the research problem is embodied in answering the following principal question:

- To what extent is Jordanian legislation adequate in regulating the civil liability of electronic signature service providers in terms of determining its legal basis, the circumstances giving rise to such liability, and the circumstances in which it is excluded, in light of modern legislative trends?
- The following sub-questions arise from this principal question:
- What is the legal status of electronic signature service providers, and what are the principal legal and technical obligations imposed upon them?
- What is the legal basis of the civil liability of electronic signature service providers, and what forms of liability arise from breaches of these obligations?
- Under what circumstances is the civil liability of electronic signature service providers excluded, and what legal rules govern exemption therefrom?
- To what extent does Jordanian legislation provide legal protection for transacting parties in light of modern legislative trends, and what are the principal aspects requiring further development?

1.2 Research Methodology

This research adopts the descriptive, analytical, and comparative approach as the most appropriate methodology for examining the civil liability of electronic signature service providers. The descriptive approach is employed to identify the legal status of electronic signature service providers, the nature of their activities, and the legal and technical obligations imposed upon them (Alatawi, 2024). The analytical approach is also employed to analyze the legal provisions governing electronic signatures and civil liability and to determine the extent to which general and specific rules are applicable to faults that may be committed by electronic signature service providers, while evaluating the adequacy of the legal framework in this field. In addition, the comparative approach is adopted by comparing the provisions of Jordanian legislation with Egyptian legislation and the European regulation concerning trust services and electronic signatures (eIDAS), with the aim of identifying areas of agreement and divergence and drawing upon comparative legislative solutions in assessing the legal regulation of the civil liability of electronic signature service providers and proposing the legislative developments necessary to enhance the legal protection of transacting parties in the digital environment.

2 Legal Obligations of Electronic Signature Service Providers as a Basis for Civil Liability

Determining the scope of the civil liability of electronic signature service providers requires, first, an examination of their legal status and the nature of the role they perform within the electronic transactions system, since identifying the nature of these entities and the obligations imposed upon them constitutes the basis upon which liability is established in the event of a breach thereof. Accordingly, this section addresses the legal status of electronic signature service providers and then analyzes the principal legal and technical obligations imposed upon them by legislation, as the framework governing the exercise of their activities and enhancing trust in the digital environment (Hashemite Kingdom of Jordan, 2014).

2.1 Legal Status of Electronic Signature Service Providers and Their Role in Enhancing Trust in Electronic Transactions

Electronic signature service providers constitute the fundamental pillar of the electronic authentication system, as legal recognition of an electronic signature is not achieved merely through the use of technical means but is linked to the existence of an entity responsible for verifying the identity of transacting parties, issuing authentication certificates, and ensuring the integrity of the data associated therewith in accordance with legal and technical requirements. Accordingly, the role of the service provider is no longer limited to providing a technical service but has come to perform a legal function consisting of enhancing trust in electronic transactions, which has prompted modern legislation to subject this activity to specific legal regulation (Telecommunications Regulatory Commission, 2015).

Jurisprudential definitions of an electronic signature service provider have varied according to the

perspective from which this activity is addressed; nevertheless, they converge in considering it a neutral entity responsible for issuing electronic authentication certificates and providing related services in a manner that ensures the validity and reliability of the electronic signature. Some legal scholars have defined it as an independent intermediary between the parties to an electronic transaction, while another approach has focused on its role in verifying the identity of the signatory and linking the signature to its holder. A third approach has regarded it as a trusted party that issues certificates attesting to the validity of facts associated with the electronic signature (Abdelrahman et al., 2026). The researchers favor the approach that broadens the concept of the service provider to encompass the issuance of authentication certificates, the services associated therewith, and the resulting legal and technical obligations, while restricting the performance of this activity to legal persons capable of providing the necessary technical and administrative requirements, given its role in safeguarding public trust in the digital environment (Arab Republic of Egypt, 2004).

This approach has been reflected in a number of legislative instruments. The UNCITRAL Model Law defines a certification service provider as a person that issues authentication certificates and provides services related to electronic signatures, while the 1999 European Directive defines it as any natural or legal person that issues authentication certificates or provides other related services. The Jordanian legislature, however, has adopted a more specific regulatory approach by defining an electronic authentication entity as an entity licensed or accredited to issue authentication certificates and provide related services. It has also authorized the Ministry of Digital Economy and Entrepreneurship to issue authentication certificates for government entities (Awaishah et al., 2026). The Egyptian legislature has followed the same approach by restricting the issuance of authentication certificates to licensed entities, reflecting the tendency of both legislatures to subject electronic signature service providers to prior regulatory oversight that ensures the availability of the minimum technical and legal requirements necessary for carrying out this activity (Arab Republic of Egypt, 2005; Arab Republic of Egypt, 2020). The researchers consider that this regulatory framework provides greater protection for electronic transactions than the framework contained in the UNCITRAL Model Law because of the safeguards it provides concerning the technical and administrative competence of service providers.

The legal status of an electronic signature service provider is closely associated with the electronic authentication certificate, which constitutes the legal instrument for establishing the identity of the signatory and linking that identity to the electronic signature creation data, thereby enabling verification of the validity of the signature and the effectiveness of its legal consequences. (Abdelrahman et al., 2026) The function of this certificate is not limited to establishing identity; rather, it performs a fundamental role in providing the trust necessary for reliance upon electronic documents. Jordanian legislation has focused on this function by requiring that the signature be linked to its holder, that the private key remain under the holder's control, and that the signature be linked to the electronic record in a manner that reveals any alteration made thereto. However, unlike certain comparative legislations, it has not specified in detail the technical data required to be included in the authentication certificate, which limits the clarity of the scope of liability of the certificate-issuing entity in the event of a breach of its obligations (Arab Republic of Egypt, 2020).

On the basis of the foregoing, the legal status of electronic signature service providers is not founded merely upon the issuance of authentication certificates but rather upon the role they perform in building trust in electronic transactions through identity verification, ensuring data integrity, and maintaining the reliability of authentication certificates throughout their period of validity. Consequently, this status entails a set of legal and technical obligations, the breach of which constitutes the basis upon which their civil liability is established (Arab Republic of Egypt, 2004).

2.2 Legal Obligations of Electronic Signature Service Providers and Their Impact on the Protection of Electronic Transactions

The reliability of an electronic signature is not dependent solely upon the existence of a legislative framework regulating the issuance of authentication certificates; rather, it is primarily dependent upon the extent to which electronic signature service providers comply with a set of technical, security, administrative, and legal obligations that ensure the integrity of the digital environment and the continuity of trust therein. These obligations do not merely constitute regulatory requirements but represent the principal safeguard for protecting the parties to electronic transactions, since a breach thereof may undermine the evidentiary value of the electronic signature

and weaken trust in digital transactions, in addition to giving rise to the civil liability of the service provider where its constituent elements are established. Accordingly, both the Jordanian and Egyptian legislatures have sought to regulate these obligations, although they differ in the degree of detail and the mechanisms adopted for their implementation (Al-Sous, 2014).

Foremost among these obligations is the service provider's obligation to provide a secure technical infrastructure that complies with approved technical standards, as this infrastructure constitutes the foundation upon which the electronic signature system is established. The Jordanian regulation requires the service provider to use an approved electronic authentication system and to provide appropriate means for protecting the operating environment and managing public and private keys. However, it confines itself to establishing a general framework without specifying detailed technical requirements, encryption standards, or mechanisms for managing the Public Key Infrastructure (PKI). By contrast, Egyptian legislation regulates these aspects in greater detail by requiring service providers to secure servers and data centers, regulate access privileges thereto, and use specialized devices for managing electronic keys, in addition to imposing requirements relating to their storage and backup (Darawsheh, 2018; Nasri, 2021). The researchers consider that the adoption of more detailed regulation in Jordanian legislation would enhance the level of protection and increase the reliability of the electronic signature system.

The protection of the technical infrastructure is closely linked to the obligation to maintain data confidentiality, as the service provider retains sensitive data relating to users' identities, electronic keys, and authentication certificate records, which requires it to take the necessary measures to prevent their unlawful disclosure or access thereto by third parties. Jordanian legislation requires the confidentiality of beneficiaries' data to be maintained and imposes penalties for breach of this obligation that may extend to the revocation of the license. Egyptian legislation, by contrast, regulates this obligation more extensively by requiring service providers to establish written information security policies, implement technical protection measures, and conduct periodic security reviews and tests, thereby providing greater protection for transacting parties and reducing the risks of data breaches or misuse (Darawsheh, 2018; Nasri, 2021).

The role of the service provider is not limited to securing systems and data but extends to ensuring the continuity of their operation and their subjection to legal oversight. Accordingly, the Jordanian regulation refers to the necessity of providing backup mechanisms and contingency plans and complying with the provisions of the Electronic Transactions Law and the instructions issued pursuant thereto. However, it does not precisely specify the standards for implementing these obligations or the mechanisms for restoring services in the event of disruptions, nor does it expressly require independent security audits or periodic training of personnel in cybersecurity and digital incident management. By contrast, Egyptian legislation adopts a more detailed regulatory framework by linking the continuation of licensing to compliance with technical and regulatory requirements and establishing rules concerning alternative data centers and service restoration procedures, reflecting a more stringent approach to the supervision of service providers (Darawsheh, 2018; Nasri, 2021).

This regulation also extends to administrative and legal obligations, whereby the service provider is required to issue authentication certificates in accordance with approved procedures, retain the records and data relating thereto, and enable the competent authority to exercise oversight over them. Jordanian legislation requires such records to be retained without specifying in detail the period for which they must be retained or the mechanisms for their management, whereas Egyptian legislation establishes more precise rules concerning the method of retention and the procedures for protection and oversight, thereby contributing to preserving the integrity and evidentiary value of such records in the adjudication of disputes (Alrfoua et al., 2026; Al-Khraisat et al., 2026).

The service provider is also required to take the necessary measures to address violations and protect beneficiaries by providing mechanisms for receiving complaints, correcting errors, and handling objections relating to authentication certificates, in addition to complying with the principles of transparency and disclosure regarding operating policies, terms of use, and certificate specifications. The researchers observe that Jordanian legislation recognizes these obligations in general terms, whereas Egyptian legislation provides more extensive provisions concerning the procedures for their implementation and links them to regulatory oversight and administrative sanctions, thereby enhancing the protection of transacting parties and increasing the level of trust in the services provided (Darawsheh, 2018; Nasri, 2021).

These obligations are manifested in practice through the essential services provided by the service provider, foremost among which are the issuance of electronic authentication certificates, the management of signature keys, the retention of verification records, and the suspension or revocation of certificates when the conditions governing their validity cease to exist. The authentication certificate constitutes the principal instrument that confers legal status upon the electronic signature. Accordingly, the Jordanian legislature requires such certificates to be issued through the competent entities, whereas Egyptian legislation subjects them to more detailed technical rules concerning identity verification and the standards to be observed when issuing them, in addition to regulating procedures for key management, record retention, revocation, and notification in greater detail (Darawsheh, 2018; Nasri, 2021). The researchers consider that introducing more detailed regulation of these aspects into Jordanian legislation would standardize the level of protection among service providers, facilitate the assessment of the extent of their compliance with the requisite professional standard of care, and enhance trust in electronic transactions (Awaisheh et al., 2025).

The researchers conclude that the technical, security, administrative, and legal obligations borne by electronic signature service providers constitute an integrated framework aimed at ensuring the reliability of electronic signatures and protecting digital transactions. They also constitute the basis upon which their civil liability is established, since a breach of any of these obligations may cause harm to beneficiaries or to third parties relying upon an authentication certificate, thereby paving the way for examining the legal basis and forms of such liability in the following section (Al-Far, 2016).

3 Legal Basis and Forms of Civil Liability of Electronic Signature Service Providers

After determining the legal status of electronic signature service providers and the obligations governing their activities, it becomes necessary to identify the legal basis of the civil liability that may arise from breaches of such obligations. This issue assumes particular importance in view of the technical nature of electronic signature services and the broad range of persons who may be affected by them, which requires a distinction to be drawn between contractual liability and tortious liability, together with an examination of the adequacy of both general and specific rules in regulating such liability.

3.1 Contractual Liability of Electronic Signature Service Providers

Contractual liability constitutes the legal framework governing the relationship between the electronic signature service provider and the beneficiary of the service, as it arises upon the conclusion of a valid contract under which the provider undertakes to provide electronic authentication services in accordance with the agreed legal and technical requirements. This contract gives rise to reciprocal obligations, foremost among which are the issuance of valid authentication certificates, verification of the identity of the certificate applicant, maintenance of data confidentiality, and management of the certificate life cycle, including its updating, suspension, or revocation where the legal grounds for doing so are established. If the provider breaches any of these obligations without proving the existence of an external cause preventing their performance, contractual liability is incurred in accordance with the general rules of civil liability (Al-Sanhouri, 2009).

Such liability is based on the existence of three elements: contractual fault, damage, and a causal relationship between them. Contractual fault consists of a breach of an obligation arising from the contract, whether through non-performance, defective performance, or delayed performance, resulting in harm to the beneficiary or undermining the trust upon which electronic authentication services are based. Given the technical nature of this activity, the assessment of fault should not be based on the standard of an ordinary person, but rather on that of a specialized professional who is required to exercise a high degree of care commensurate with the nature of the services provided (Mohammed, 2020).

The assessment of fault is linked to the nature of the obligation borne by the service provider, as civil law distinguishes between an obligation to achieve a result and an obligation to exercise due care (Yas et al., 2026). The researchers consider that most obligations performed by an electronic signature service provider are closer to obligations to achieve a result, particularly those relating to the issuance of authentication certificates and the accuracy of the data contained therein, because the primary purpose of the contractual relationship is to enable the beneficiary to rely upon a valid and trustworthy certificate (Rukba et al., 2025). Accordingly, the issuance of a certificate containing inaccurate information or information inconsistent with reality is sufficient to establish

liability unless the provider proves that the failure to achieve the required result was attributable to an external cause beyond its control. As for obligations relating to the periodic monitoring of certificates, maintenance of systems, and suspension or revocation of certificates, although they may appear to constitute obligations to exercise due care, the researchers consider that, in practice, they are closer to obligations to achieve a result, given the fundamental role they perform in maintaining the reliability of electronic signatures and the stability of digital transactions (Dawwas, 2010).

Contractual liability is clearly manifested where the service provider breaches its fundamental obligations, such as issuing an authentication certificate on the basis of inaccurate data, breaching the duty to maintain data confidentiality, or delaying the suspension or revocation of a certificate despite the existence of legal or technical grounds requiring such action (Awaishah, 2023). These obligations constitute the foundation upon which trust in electronic signatures is based; consequently, their breach gives rise to the provider's liability where damage is caused to the beneficiary (Al-Zarqa, 1963).

Damage constitutes the second element of contractual liability and refers to the harm suffered by the beneficiary as a result of the service provider's breach of its obligations, whether in the form of direct financial loss or impairment of a legitimate interest arising from reliance upon a defective or inaccurate authentication certificate (Alhasan, 2025). For compensation to be awarded, the damage must be direct and certain, and the beneficiary must prove its occurrence, while compensation remains, in principle, limited to damage constituting a natural consequence of the breach of contract, unless the fault is accompanied by fraud or gross negligence (Hashemite Kingdom of Jordan, 1976).

Liability is completed by the existence of a causal relationship between the contractual fault and the damage, such that the damage is a direct consequence of the service provider's breach of its obligations. If the provider proves that the damage resulted from an external cause beyond its control, liability is excluded (Awaishah et al., 2026). The scope of this liability is limited to persons having a direct contractual relationship with the provider. By contrast, a third party who relies upon an authentication certificate in the absence of a contractual relationship is legally protected under the rules of tortious liability (Hashemite Kingdom of Jordan, 1976).

The researchers conclude that the contractual liability of electronic signature service providers is characterized by particular features arising from the technical nature of electronic authentication services, making most of the fundamental obligations borne by the provider, particularly those relating to the accuracy of certificate data, confidentiality of information, and management of the certificate life cycle, closer to obligations to achieve a result than to obligations to exercise due care. This justifies the application of a stricter standard of liability and requires legislative development to define more precisely the standards of professional fault in this field, thereby enhancing the protection of beneficiaries and trust in electronic transactions (Dawwas, 2010).

To illustrate the distinctions between the forms of civil liability that may arise on the part of an electronic signature service provider, Table (1) sets out the legal basis of each form and the principal circumstances in which liability arises, as a preliminary step toward examining the characteristics of tortious liability in the following section.

Table 1. Forms of Civil Liability of Electronic Signature Service Providers

Form of Liability	Legal Basis	Principal Cases of Application
Contractual Liability	The contract concluded between the service provider and the beneficiary	Issuing a certificate containing inaccurate data; breach of confidentiality; delay in suspending or revoking the certificate; breach of contractual obligations
Tortious Liability	General rules governing liability for harmful acts	Issuing a misleading certificate that causes damage to third parties; breach of protective duties; failure to verify data; damage suffered by third parties relying upon the certificate

It is evident from Table (1) that the distinction between contractual and tortious liability is not related solely to the nature of the fault but is primarily based on the nature of the legal relationship between the service

provider and the injured party, which necessitates an examination of tortious liability and its rules in the field of electronic signature services.

3.2 Tortious Liability of Electronic Signature Service Providers

The liability of electronic signature service providers is not limited to contractual relationships with beneficiaries but extends to third parties who, in good faith, rely upon electronic authentication certificates without having a direct contractual relationship with the provider (Naseir et al., 2026). The significance of this liability arises from the fact that the effects of an authentication certificate are not confined to the parties to the contract but extend to every person who relies upon it in verifying the identity of the signatory and the validity of the data associated with the electronic signature. Tortious liability therefore constitutes the appropriate legal mechanism for compensating third parties for damage resulting from breaches of the service provider's duties (Al-Far, 2016). This liability is based on the general rules governing harmful acts; however, Jordanian and Egyptian legislation differ with respect to its legal foundation. The Jordanian legislature adopts the concept of causing harm and does not require the person causing the damage to possess discernment or legal capacity; rather, any act causing harm to another gives rise to an obligation to provide compensation where damage occurs (Alsaraireh et al., 2026). This approach is derived from Islamic jurisprudence and is aimed at providing broader protection to the injured party. By contrast, the Egyptian legislature bases liability on fault and requires the harmful act to have been committed by a person possessing discernment, reflecting the influence of civil law systems of Latin origin. The researchers consider that this distinction reflects two different legislative philosophies: while Jordanian law gives priority to reparation of harm, Egyptian law links liability to the existence of fault as the basis of civil accountability (Hashemite Kingdom of Jordan, 1976; Mohammed, 2020).

In the field of electronic signature services, tortious fault occurs whenever there is a breach of the general legal duty imposed upon the service provider to ensure the reliability of authentication certificates and the integrity of the systems through which they are issued (Al-Zarqa, 1963). This may arise through the issuance of certificates based on inaccurate data, failure to verify the identity of the certificate applicant, negligence in protecting the technical infrastructure and managing electronic keys, or failure to suspend or revoke a certificate after the conditions governing its validity have ceased to exist, thereby causing damage to third parties. This obligation derives from the general legal duty rather than from a contractual relationship, which justifies the establishment of tortious liability upon its breach (Al-Far, 2016).

This is consistent with the distinction adopted by the Jordanian Civil Code between direct causation of harm and indirect causation of harm. In cases of direct harm, liability arises upon the occurrence of damage, whereas in cases of indirect causation, the act must be accompanied by wrongful conduct or intent, or must by its nature lead to the occurrence of the damage. This distinction assumes particular importance in electronic signature services because most damage suffered by third parties results from failures in verification, protection, or oversight procedures, making the provider liable as the indirect cause of the damage where a failure to perform professional duties is established (Hashemite Kingdom of Jordan, 1976; Mohammed, 2020).

Tortious liability does not arise unless such breach results in direct and certain damage, represented by the loss suffered by a third party as a consequence of relying upon an inaccurate authentication certificate, such as the invalidation of an electronic transaction, the incurrence of financial obligations, or the loss of rights that would not have occurred but for the fault committed by the service provider (Hashemite Kingdom of Jordan, 1976). A causal relationship between the fault and the damage must also be established, such that the damage is a direct consequence of the provider's breach of its duties (Alhasan & Awaisheh, 2024). Liability is excluded if it is established that the damage resulted from an external cause, such as force majeure, the act of a third party, or the fault of the injured party. This approach achieves a balance between protecting injured parties and preventing the service provider from being held liable for damage falling outside its sphere of control (Mohammed, 2020).

In this context, an issue arises concerning the burden of proving fault, particularly in view of the complex technical nature of electronic signature services, as it may be difficult for the injured party to establish technical deficiencies (Al-Far, 2016; Al-Zarqa, 1963). The researchers consider that the particular nature of this activity requires the conduct of the service provider to be assessed according to the standard of a specialized professional, such that non-compliance with technical or security standards constitutes evidence of fault where

a connection with the damage is established. The burden should also be placed upon the service provider to prove compliance with such standards, since the technical evidence and data required to establish the integrity of the relevant procedures are within its possession (Alhasan, 2026).

The establishment of tortious liability on the part of an electronic signature service provider does not necessarily mean that it bears sole responsibility for all damage suffered by third parties. Depending on the circumstances of each case, liability may also extend to the competent licensing and supervisory authority in view of its role in verifying that service providers satisfy the applicable legal and technical requirements and in monitoring their continued compliance therewith (Alhasan et al., 2026). If it is established that such authority granted a license despite the failure to satisfy the statutory requirements, or failed to exercise the supervision required by law, and such failure caused the damage, it may be held liable in accordance with the general rules of legal liability where its constituent elements are established. This does not preclude the liability of the service provider where its fault is also established, which may result in joint liability depending on the circumstances of the case (Darawsheh, 2018; Hashemite Kingdom of Jordan, 1976).

The researchers conclude that tortious liability constitutes the principal legal safeguard for protecting third parties who rely upon electronic authentication certificates in the absence of a contractual relationship with the service provider. Comparative analysis also shows that Jordanian legislation provides broader protection to injured parties through its adoption of the concept of causing harm, whereas Egyptian legislation is based on the concept of fault. Nevertheless, both systems share the requirements that damage must occur and a causal relationship must be established, thereby confirming the importance of developing the legal framework in a manner that keeps pace with the technical nature of electronic signature services and enhances trust in digital transactions.

4 Regulation of the Exclusion of Civil Liability of Electronic Signature Service Providers

The regulation of the civil liability of electronic signature service providers is not complete merely by identifying the grounds upon which such liability arises; rather, it also requires the determination of the circumstances in which liability is excluded or may be limited, in order to achieve a balance between protecting transacting parties and avoiding the imposition upon the service provider of liability for damage falling outside its control. Accordingly, this section addresses the circumstances in which liability is excluded, the rules governing exemption therefrom, and the effect of an external cause in severing the causal relationship, while drawing upon comparative approaches in evaluating Jordanian regulation.

4.1 Exclusion of Civil Liability of Electronic Signature Service Providers

The liability of electronic signature service providers is not absolute but is subject to the general rules of civil liability, which permit the debtor to deny liability where it proves the absence of one of its constituent elements or the existence of a legal ground preventing such liability from being attributed to it (Pérez Carrillo & Alhasan, 2026). This issue assumes particular importance in the digital environment in view of the complex technical nature of electronic signature services and the specialized technical and security obligations they entail, which may expose the service provider to liability claims despite its compliance with the prescribed professional standards (Awaisheh & Al-Dabbas, 2024). Accordingly, liability is not excluded merely by denying fault; rather, it requires proof that the provider has exercised the requisite technical and professional care, complied with all legal and regulatory requirements, and that the damage suffered by the beneficiary or a third party is not attributable to any failure on its part (Al-Zarqa, 1963; Mohammed, 2020).

In this context, the denial of liability is primarily based on rebutting the presumption of fault that may arise from a breach of the professional obligations of the service provider. Under the general rules of Jordanian and Egyptian law, the provider is required to exercise the care of an ordinary person where the obligation concerns the exercise of due care rather than the achievement of a result. However, the researchers consider that the application of this standard in the field of electronic signature services should not be confined to the care expected of an ordinary person but should be interpreted in light of the nature of the activity as a professional technical activity. Accordingly, the provider's conduct should be assessed according to the standard of care expected of an expert or a specialized technical institution, given the advanced technical expertise and high information security and cybersecurity standards required by such services. Consequently, the service provider

may deny liability only where it proves compliance with all recognized technical and regulatory standards and the adoption of the preventive measures necessary to avert the occurrence of damage (Al-Far, 2016; Al-Zarqa, 1963).

This obligation is manifested in practice through a set of duties that constitute the basis of trust in the electronic signature system, foremost among which is the verification of the accuracy of the data contained in the authentication certificate before its issuance, since such data constitute the basis upon which transacting parties rely in verifying the identity of the signatory and the validity of the electronic signature. The service provider is therefore required to examine the submitted documents and verify their authenticity through appropriate technical and legal means (Alhasan, 2025). If forgery or inaccuracy in the data becomes apparent, the provider must refrain from issuing the certificate. However, where the documents appear authentic and do not reasonably disclose any forgery, liability is excluded if the provider proves that the required verification procedures have been fulfilled. This obligation also extends to updating the data contained in certificates and maintaining their accuracy throughout their period of validity, since continued reliance upon outdated data may cause harm to transacting parties and establish the provider's liability (Al-Far, 2016; Al-Sous, 2014).

Of no less importance is the service provider's obligation to maintain the confidentiality of the data obtained in the course of providing its services. Jordanian and Egyptian legislation provide specific protection for personal information and electronic signature creation data and prohibit their use or disclosure for purposes other than those for which they were collected (Awaisheh, Alkhamaiseh, et al., 2024). However, the researchers consider that this obligation does not amount to an obligation to achieve a result, since the service provider cannot be required to guarantee the absolute impossibility of any electronic breach. Rather, it is required to exercise the care of a specialized expert by applying the most advanced encryption methods, updating protection systems, and complying with international cybersecurity standards. Accordingly, liability is excluded where the provider proves that the disclosure or breach of data resulted from an external cause that could neither have been foreseen nor prevented despite the adoption of all necessary security measures (Al-Sous, 2014; Darawsheh, 2018).

The scope of the obligations whose performance must be established by the service provider also extends to the management of the authentication certificate life cycle, including its suspension or revocation immediately upon the occurrence of legal or technical grounds requiring such action, such as the discovery of forged data, loss of control over the private key, alteration of the signatory's essential data, or the cessation of any condition governing the validity of the certificate (Awaisheh, Al-Hassan, et al., 2024). The obligation to take such measures in a timely manner constitutes one of the most important manifestations of professional care, since continued reliance upon a certificate that has lost its legal validity may cause third parties to rely upon it and enter into transactions lacking reliability, thereby giving rise to the provider's liability where delay or negligence is proven to have caused the damage. Conversely, where the provider proves that it complied with the prescribed legal and technical procedures and took the appropriate decision as soon as the relevant ground arose, liability is excluded due to the absence of fault (Al-Far, 2016; Al-Sous, 2014).

The service provider may not disclaim liability on the ground that the fault was committed by one of its employees, since the general rules under Jordanian and Egyptian legislation establish the liability of a principal for damage caused by its subordinate in the course of or by reason of the performance of employment duties (Awaisheh, 2023). Accordingly, the issuance by an employee of an inaccurate authentication certificate, failure to verify data, or breach of protection procedures is, in principle, regarded as fault attributable to the service provider itself in its capacity as the legal person responsible for managing the activity (Al-Zubi et al., 2024). The researchers consider that such liability should remain presumed, so that the provider bears responsibility for the faults of its employees, given that it is best positioned to select and supervise them and is also better able to bear the professional risks associated with the activity. This provides effective protection for injured parties and enhances trust in electronic authentication services (Hashemite Kingdom of Jordan, 1976; Mohammed, 2020). The denial of liability is not limited to rebutting fault but may also be achieved by severing the causal relationship through proof that the damage resulted from an external cause beyond the provider's control. Foremost among such causes is force majeure, which renders the performance of the obligation absolutely impossible, provided that the event is unforeseeable, unavoidable, and beyond the provider's control (Althunibat et al., 2025). However, the researchers consider that the scope of force majeure in the field of electronic signature services should remain

narrowly construed because the nature of this activity requires the provider to anticipate most technical risks and adopt the necessary precautions to address them. Accordingly, many technical failures and cyberattacks are not, in themselves, sufficient to constitute force majeure unless they are exceptional and incapable of being foreseen or resisted, such as natural disasters that destroy data centers or sovereign decisions that render performance of the obligation absolutely impossible (Hashemite Kingdom of Jordan, 1976; Mohammed, 2020).

The provider may also invoke the act of a third party where such act is external to its activity and could neither have been foreseen nor prevented (Alhasan & Awaisheh, 2024). However, the success of such a defense remains dependent upon proof that the damage did not result from deficiencies in protection systems or non-compliance with the required security standards. Legal Jurisprudence therefore distinguishes between the act of an external third party, which may sever the causal relationship, and the act of one of the provider's employees, which does not exempt the provider from liability because employee faults fall within the scope of its legal responsibility. The researchers consider that cyberattacks do not constitute an external cause merely because they occur; rather, it must be determined whether they could have been prevented or their effects mitigated through appropriate technical measures. If deficiencies in protection systems are established, the provider's liability remains notwithstanding the intervention of a third party (Al-Far, 2016; Mohammed, 2020).

The fault of the injured party may also constitute a ground for excluding liability, whether it takes the form of negligence by the signatory in safeguarding the private key, the provision of inaccurate data to the service provider, or failure by the relying party to verify the validity of the authentication certificate or the restrictions contained therein before relying upon it. The UNCITRAL Model Rules attach particular importance to this obligation by requiring both the signatory and the relying party to exercise reasonable care in protecting signature creation means and verifying the validity of the certificate (Alkuwari & Abdelrahman, 2026). The researchers consider that the effect of the injured party's fault depends upon the extent of its contribution to the occurrence of the damage (Awaisheh, Odeibat, et al., 2026). If it constitutes the sole and direct cause of the damage, the service provider is completely exempted from liability. However, if the fault of the injured party combines with that of the provider in causing the damage, liability is apportioned between them according to the extent of each party's contribution to its occurrence, thereby achieving a balance between protecting the injured party and avoiding the imposition upon the service provider of liability for damage for which it was not solely responsible (Mohammed, 2020; United Nations, 2001).

The researchers conclude that the exclusion of the civil liability of electronic signature service providers remains an exception that applies only where the provider proves full compliance with the legal, technical, and security obligations imposed by the nature of its activity or establishes that the damage resulted from an external cause beyond its control. It is also evident that the digital environment requires a stricter interpretation of the applicable standard of care, thereby making the scope of exemption from liability narrower than that applicable in traditional civil relationships and, in turn, enhancing the protection of transacting parties and reinforcing trust in electronic signature services (Awaisheh, Al-Awaysheh, et al., 2026).

4.2 Rules Governing Exemption from Civil Liability in Light of Comparative Legislation

An agreement modifying the effects of contractual liability constitutes one of the traditional applications of the principle of freedom of contract, as contracting parties may, in principle, agree to increase, reduce, or limit liability, and such agreement may extend to the total or partial exemption therefrom, provided that it does not contravene rules of public order or public morals. This principle applies to electronic signature service contracts, in which the service provider may include clauses limiting its liability for certain potential damage or restricting such liability to specific circumstances, with the aim of reducing the risks associated with the technical nature of the activity it performs (Al-Awaysheh et al., 2026). However, the particular nature of electronic authentication services, which are founded upon trust and reliance by transacting parties, renders contractual freedom in this field subject to stricter legal controls than those applicable to traditional civil contracts (Hashemite Kingdom of Jordan, 1976; Mohammed, 2020).

In this context, it is observed that Jordanian legislation does not expressly provide for the permissibility of agreeing to exemption from contractual liability. Nevertheless, such an approach may be implicitly inferred from the provisions of the Civil Code, which permit contracting parties to regulate the effects of their contractual relationship within limits that do not conflict with mandatory provisions, public order, or good faith. By contrast,

the Egyptian legislature addresses this matter more explicitly by permitting an agreement exempting the debtor from contractual liability, while excluding liability arising from fraud or gross fault. This reflects an approach that balances respect for contractual autonomy with the provision of a minimum level of protection for the injured party, confirming that the right of an electronic signature service provider to include clauses limiting its liability in its contracts is not absolute but is subject to the restrictions established by the general rules and to judicial scrutiny (Hashemite Kingdom of Jordan, 1976; Mohammed, 2020).

The first of these restrictions is the prohibition against exemption from liability arising from fraud or gross fault, on the basis that both constitute a departure from the requirements of good faith and affect the very essence of the contractual obligation. This restriction assumes particular importance in the field of electronic signature services (Naseir et al., 2026) . Issuing an authentication certificate on the basis of data known by the provider to be inaccurate, gross negligence in protecting key management systems, or the use of technical means whose inadequacy has been established does not constitute merely an ordinary breach of an obligation but represents a direct impairment of the trust upon which the electronic authentication system is founded. Accordingly, any clause intended to exempt the service provider from liability in such circumstances is without legal effect, and its liability remains established notwithstanding the inclusion of such a clause in the contract (Al-Far, 2016; Hashemite Kingdom of Jordan, 1976; Mohammed, 2020).

To demonstrate the principal legal restrictions governing agreements on exemption from civil liability and the extent to which they are regulated under Jordanian and Egyptian legislation, Table (2) sets out the principal restrictions and the areas of agreement and difference between the two systems, as the principal rules limiting the freedom of an electronic signature service provider to exclude or restrict its civil liability.

Table 2. Legal Restrictions on Exemption from Civil Liability under Jordanian and Egyptian Legislation

Exemption Case	Jordanian Legislation	Egyptian Legislation
Agreement to limit liability	Permissible within the limits of the general rules and provided that public order is not violated	Permissible under the Civil Code subject to statutory restrictions
Exemption from liability for fraud	Not permissible	Not permissible
Exemption from liability for gross fault	Not permissible	Not permissible
Exemption from liability for employees' faults	Subject to the general rules governing the liability of a principal for the acts of its subordinate	Subject to the legal rules governing the debtor's liability for its subordinates
Requirement of transparency and disclosure	Inferred from the general rules and the principle of good faith	Requires exemption clauses to be clear and disclosed to the transacting party
Violation of public order	Results in the invalidity of the exemption clause	Results in the invalidity of the exemption clause

It is evident from Table (2) that Jordanian and Egyptian legislation agree on subjecting exemption clauses to a set of restrictions aimed at protecting transacting parties and preventing the misuse of contractual freedom, although they differ in the degree of detail with which such restrictions and their regulatory mechanisms are addressed (Alsaraireh, Awaisheh, et al., 2026). Accordingly, the mere inclusion of an exemption clause in a service contract is insufficient for it to produce legal effects; rather, its legality, its relationship to the nature of the obligation, and the extent of its impact on the beneficiary's rights must be examined.

This restriction extends to the fundamental obligations upon which the service contract is based, as an exemption clause may not deprive the contract of its substance or deny the beneficiary the principal purpose for which the contract was concluded. Such obligations include, in particular, verifying the identity of the certificate applicant, ensuring the accuracy of the data contained therein, maintaining their confidentiality, securing the technical infrastructure upon which the electronic authentication system is based, and suspending or revoking the certificate when the conditions governing its validity cease to exist (Al-Kasassbeh et al., 2024). Accordingly, any clause exempting the service provider from liability for breach of these obligations loses its legitimacy because it undermines the foundation of the contractual relationship and weakens trust in electronic

transactions (Alsaraireh, Alrfoua, et al., 2026). The researchers consider that this approach is consistent with the particular nature of electronic signature services, since the subject matter of the contract is not limited to the provision of a technical service but extends to providing the trust and reliability upon which transacting parties rely when concluding their legal transactions (Al-Far, 2016; Al-Sous, 2014; Al-Zarqa, 1963).

In this context, a question arises as to whether the service provider may be exempted from liability for the faults of its employees (Alayaydeh et al., 2025). As a general rule, the service provider, being the entity that selects, supervises, and directs its employees, remains liable for faults committed by them during or by reason of the performance of obligations associated with the service. Moreover, the nature of electronic authentication services requires the service provider to be regarded as an integrated institution rather than as a group of separate individuals, because the transacting party relies upon the competence and reliability of the licensed entity rather than upon the personal performance of the employee carrying out the relevant procedure. Accordingly, exempting the provider from liability for employee faults associated with the issuance of certificates, verification of data, or protection of systems would weaken the legal protection afforded to transacting parties, particularly where the fault relates to a fundamental obligation or reaches the level of fraud or gross fault (Hashemite Kingdom of Jordan, 1976; Mohammed, 2020).

The restrictions are not confined to substantive considerations but also extend to requirements of transparency and disclosure. For an exemption clause to be effective, it must be clear, specific, and made available to the transacting party before the conclusion of the contract, thereby enabling that party to understand the scope of the service provider's liability and the limits of the risks that may be borne. The UNCITRAL Model Law on Electronic Signatures attaches particular importance to this matter by emphasizing the need to enable the relying party to ascertain any limitations imposed upon the scope of use of the certificate or the liability of the certification service provider (Awaishah, Al-Abbadi, et al., 2025). This obligation assumes greater significance in the digital environment, where direct negotiation is often absent and service terms are contained in standard-form contracts prepared in advance by the service provider, thereby placing the user in a weaker contractual position. Accordingly, an exemption clause that is ambiguous, inconspicuous, or not made reasonably available to the beneficiary before contracting should not be invoked against that beneficiary (Mohammed, 2020; United Nations, 2001).

On the basis of the foregoing, the researchers conclude that exemption from liability in electronic signature service contracts remains an exception of limited scope, governed by considerations relating to the protection of trust in digital transactions to the same extent as by principles of contractual freedom (Awaishah, Alsaraireh, et al., 2025). Accordingly, such exemption may not extend to cases of fraud, gross fault, or breach of fundamental obligations, nor may it be used as a means of avoiding liability for employee faults directly connected with the performance of the service. The exemption clause must also be clear, specific, and disclosed to the transacting party before the conclusion of the contract and must not disturb the contractual balance or prejudice the rights of the weaker party. This demonstrates that the development of legal protection requires a more detailed legislative framework defining the scope and limits of exemption clauses in electronic signature service contracts in a manner consistent with the technical nature of these services and conducive to enhancing trust in digital transactions.

5 Conclusion

It is concluded in the study that the civil liability of electronic signature service providers constitutes one of the fundamental pillars for ensuring trust in electronic transactions, given the pivotal role performed by the service provider in identity verification, the issuance of authentication certificates, and the protection of the integrity of the digital environment. It is also demonstrated that the technical and professional nature of this activity requires a legal approach that goes beyond the traditional applications of civil liability, in a manner that achieves a balance between protecting transacting parties and avoiding the imposition upon the service provider of liability for damage falling outside its control. In light of the foregoing, the Jordanian regulation of civil liability is analyzed in the study, and the principal aspects requiring further development are highlighted, leading to a set of findings and recommendations that may contribute to strengthening the legal framework governing electronic signature services and ensuring that it keeps pace with rapid technological developments.

5.1 Findings

- It is demonstrated in the study that an electronic signature service provider performs a legal and technical function that extends beyond the mere issuance of authentication certificates, as it constitutes the fundamental pillar for building trust in electronic transactions and ensuring their reliability.
- It is shown in the study that the technical, security, and administrative obligations borne by the service provider constitute the basis upon which its civil liability is established and that a breach of any of these obligations may give rise to liability where its constituent elements are established.
- It is concluded in the study that the liability of an electronic signature service provider takes two forms: contractual liability toward a beneficiary who has a contractual relationship with the provider, and tortious liability toward a third party who relies upon an authentication certificate without having a direct contractual relationship with the provider.
- It is revealed in the study that most of the fundamental obligations of the service provider, particularly those relating to the accuracy of authentication certificate data and the management of their life cycle, are closer to obligations to achieve a result than to obligations to exercise due care, given the nature of the activity and its direct impact on the stability of electronic transactions.
- It is shown in the study that Jordanian regulation is characterized by generality in a number of aspects relating to technical standards, electronic key management, record retention, and procedures for the suspension and revocation of certificates, compared with comparative legislation that has adopted more detailed regulation.
- It is demonstrated in the study that exemption from civil liability may not extend to cases of fraud, gross fault, or breach of the fundamental obligations upon which the service provider's activity is based and that such exemption is also subject to the requirements of transparency, good faith, and compliance with public order.
- It is concluded in the study that an external cause does not exempt the service provider from liability unless it is established that it was beyond the provider's control, could neither have been foreseen nor prevented, and constituted the direct cause of the damage, with the scope of application of this defense being narrowly construed in the digital environment.

5.2 Recommendations

- It is recommended that Jordanian legislation be amended to provide more detailed regulation of the civil liability of electronic signature service providers, clearly defining the nature of the obligations borne by the provider and the consequences of breaches thereof.
- It is recommended that mandatory technical standards be established to regulate the issuance of electronic authentication certificates, the management of electronic keys, record retention, and procedures for the suspension and revocation of certificates, thereby enhancing the reliability of electronic signature services.
- It is recommended that the standard of professional care required of electronic signature service providers be more clearly stipulated in a manner consistent with the professional and technical nature of this activity.
- It is recommended that the provisions governing the burden of proof in electronic signature disputes be developed in a manner that achieves a balance between the positions of the parties to the dispute and takes into account the particular nature of technical evidence.
- It is recommended that exemption clauses relating to civil liability be expressly regulated by legislation, with their scope and governing rules clearly defined, and that reliance upon such clauses be prohibited in cases of fraud, gross fault, or breach of fundamental obligations.
- It is recommended that comparative legislative experiences be utilized, particularly in the regulation of technical obligations and mechanisms for supervising electronic signature service providers, thereby contributing to the development of the Jordanian legislative environment and enhancing trust in digital transactions.

References

- Abdelrahman, A., Awaisheh, S. M., Awaisheh, S. M., & Al-Thnaibat, O. H. A. (2026). Speaking—and silencing—the Constitution: A semiotic analysis of Jordan's Constitutional Court judgments (2025). *International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique*. <https://doi.org/10.1007/s11196-026-10462-5>
- Alatawi, O. D. (2024). The Saudi Arabian legal system's approach to white-collar crimes: Challenges and potential reforms. *Cogent Social Sciences*, 10(1). <https://doi.org/10.1080/23311886.2024.2413622>
- Alatawi, O. D. (2025). Combating corruption and promoting economic resilience: Legal and institutional reform in Saudi Arabia. *Humanit Soc Sci Commun*, 12, 1597. <https://doi.org/10.1057/s41599-025-05873-x>
- Al-Awaysheh, S. M., Alsaraireh, N., Smairan, A. M., Awaisheh, S. M., Awaisheh, S. M., & Al-Khraisat, W. M. M. (2026). Medical liability for missing the opportunity for a patient's recovery or survival in Jordanian legislation: An analytical legal study. *Genetics and Molecular Research*. <https://doi.org/10.4238/ag42af18>
- Alayaydeh, H. A., Awaisheh, S. M., Al-Taani, M., Al-Dabbas, N. A., Alqudah, A. M.-A., & Awaisheh, S. M. (2025). The problem of establishing civil liability for harmful effects of smart robots. *Indian Journal of Information Sources and Services*, 15(4), 31–39. <https://doi.org/10.51983/ijiss-2025.IJISS.15.4.04>
- Al-Far, A. Q. (2016). *Sources of obligations: Sources of personal rights under civil law* (8th ed.). Dar Al-Thaqafa.
- Alhasan, T. K. (2025). The role of blockchain in modernizing FIDIC contracts: Opportunities and challenges. In R. K. Hamdan (Ed.), *Tech fusion in business and society* (Studies in Systems, Decision and Control, Vol. 234, pp. 565–573). Springer. https://doi.org/10.1007/978-3-031-84636-6_49
- Alhasan, T. K. (2026). Governing the black box in adjudication: Policy frameworks for algorithmic transparency in international arbitration. *Social Sciences & Humanities Open*, 14, Article 103109. <https://doi.org/10.1016/j.ssaho.2026.103109>
- Alhasan, T. K., Alqaisi, M., & Alabdallat, F. (2026). Governing automated credit after explainability: From transparency to contestability. *Social Sciences & Humanities Open*, 14, Article 103577. <https://doi.org/10.1016/j.ssaho.2026.103577>
- Alhasan, T. K., & Awaisheh, S. M. (2024). The right of public employee to defend disciplinary penalty in Jordan. *International Journal of Public Law and Policy*, 10(2), 190–203. <https://doi.org/10.1504/IJPLAP.2024.137783>
- Alhrerat, K. A., Alnsour, T. M. Q., Almasarweh, S. I. M., Alqudah, A. M.-A., Awaisheh, S. M. A., & Awaisheh, S. M. (2025). Safeguarding electronic signatures in Jordan: Legal foundations and enforcement challenges. *Indian Journal of Information Sources and Services*, 15(4), 302–308. <https://doi.org/10.51983/ijiss-2025.IJISS.15.4.34>
- Al-Kasassbeh, F. Y., Awaisheh, S. M., & Odeibat, M. A. (2024). Digital human rights in Jordanian legislation and international agreement. *International Journal of Cyber Criminology*. <https://doi.org/10.5281/zenodo.4766803>
- Al-Khraisat, W. M. M., Awaisheh, S. M., Al-Wreikat, E. I., AbuMalik, T. H. M., Alkasasbeh, A. A. M., Alrfoua, A. Y., Awaisheh, S. M., & Abdelrahman, A. (2026). Administrative justice and regulatory governance in environmental licensing: Balancing legal certainty and sustainable development in Jordan and France. *Corporate Law & Governance Review*, 8(3), 113–120. <https://doi.org/10.22495/clgrv8i3p10>
- Alkuwari, K., & Abdelrahman, A. (2026). Third-party countermeasures in cyberspace: Reconciling state practice with the law of state responsibility. *Computer Law & Security Review*, 63, Article 106396. <https://doi.org/10.1016/j.clsr.2026.106396>
- Alrfoua, A. Y., Awaisheh, S. M. A., Al-Wreikat, E. I., Al-Khraisat, W. M. M., Awaisheh, S. M., & Abdelrahman, A. (2026). The role of administrative regulatory authorities in protecting the environmental sustainability of natural resources: A legal analytical study. *Scientific Culture*, 12(1.1), 340–357. <https://doi.org/10.5281/zenodo.11425133>
- Alsalmi, M., Alatawi, O., Badran, D., Abdelhady, M., Alsherman, N., & Alrousan, E. (2026). Armed conflicts and their environmental impacts: Toward a global legal framework for promoting environmental sustainability. *Asian Journal of Water, Environment and Pollution*, 23(3), 025480366. <https://doi.org/10.36922/AJWEP025480366>
- Al-Sanhouri, A. R. A. (2009). *Al-Wasit in the explanation of civil law: Sources of obligations* (3rd ed.). Al-

- Alsaraireh, N., Alrfoua, A., Al-Khraisat, W., Awaisheh, S., Alduros, S. M. S., Alja'afreh, I., & Alkhattab, K. A. R. (2026). Special privileges enjoyed by female public service employees (leave as a model): A comparative study of Jordanian and Bahraini legislation. In R. K. Hamdan (Ed.), *Technological innovation and enhancing decision processes in modern enterprises* (Studies in Systems, Decision and Control, Vol. 631, pp. 741–751). Springer. https://doi.org/10.1007/978-3-032-04378-8_67
- Alsaraireh, N., Awaisheh, S., Alswelmieen, S., & Al-Maagbeh, M. (2026). The role of legal legislation in empowering women and supporting their participation in political life in light of Bahraini and Jordanian legislation. In *Studies in Systems, Decision and Control*. Springer. https://doi.org/10.1007/978-3-032-04378-8_61
- Al-Sous, H. L. (2014). *Electronic certification service provider* [Unpublished master's thesis]. Damascus University.
- Althunibat, A. O., Awaisheh, S. M., Al-Hobabseh, W. I., Alhendi, N. I., Samawi, R. S. F., Alamaireh, M. A. M., & Awaisheh, S. M. (2025). Market manipulation risks in contracts for difference (CFDs): Legal regulation and the Jordanian framework. *Research Journal in Advanced Humanities*, 6(4). <https://doi.org/10.58256/dt93t122>
- Al-Zarqa, M. (1963). *Islamic jurisprudence in its new form* (Vol. 2, 7th ed.). Dar Al-Fikr.
- Al-Zubi, J. K., Maaqqbeh, M., Awaisheh, S. M., & Mofleh. (2024). Progress and challenges in the legal framework of women's rights in Jordan. *International Journal of Criminal Justice Sciences*. <https://doi.org/10.5281/zenodo.19128>
- Arab Republic of Egypt. (2004). Electronic Signature Law No. 15 of 2004. *Official Gazette*, 17 (Supplement D).
- Arab Republic of Egypt. (2005). Executive Regulations of the Electronic Signature Law No. 109 of 2005. *Official Gazette*, 115.
- Arab Republic of Egypt. (2020). Decision No. 361 of 2020 amending the Executive Regulations of the Electronic Signature Law. *Egyptian Gazette*, 95.
- Awaisheh, S. M. (2023). Digital justice in Jordan: The role of virtual arbitration sessions in modernizing the legal system. *International Journal of Cyber Criminology*. <https://doi.org/10.5281/zenodo.4766609>
- Awaisheh, S. M. (2025). From paper to pixels: The legal status and challenges of electronic writing in administrative contracts—A comparative study. *Electronic Government*. <https://doi.org/10.1504/EG.2025.144726>
- Awaisheh, S. M. A., Al-Abbadi, H. S., Al-Dabbas, N. A., Hmaidan, R., Al-Khalaileh, L., & Al-Tarawneh, A. S. (2025). New claims and causes of action before the Court of Appeal in Jordanian civil procedure. *Journal of Human Security*. <https://doi.org/10.12924/johs2025.210108>
- Awaisheh, S. M., Al-Awaysheh, S. M., Awaisheh, S. M., Khashashneh, T., Bqoor, K. J., Asfour, A., & Al-Khraisat, W. M. M. (2026). The effect of artificial intelligence of the development of phishing attacks. *Social Science Forum*, 10(8), 695–714. <https://doi.org/10.10118/SSFJ/2610839>
- Awaisheh, S. M., & Al-Dabbas, N. A. (2024). The dichotomy of interests: A comparative analysis of civil and administrative lawsuits in the Jordanian legal system. *International Journal of Criminal Justice Sciences*. <https://doi.org/10.5281/zenodo.19108>
- Awaisheh, S. M., Aldalain, Z. H. I., Alhendi, N. I., Alawaysheh, A., Al-Tarawneh, A. S., Awaisheh, S. M., & Al-Khraisat, W. M. M. (2026). The role of linguistic artificial intelligence models in drafting administrative contract. *Social Science Forum Journal*, 10(7), 321–338. <https://doi.org/10.10118/SSFJ/2610717>
- Awaisheh, S., Al-Hassan, T., & Mansour, A. (2024). The status of digital evidence in administrative litigation. *Al-Balqa Journal for Research and Studies*, 27(3), 42–55. <https://doi.org/10.35875/pgdx2798>
- Awaisheh, S. M., Alkhamaish, M. A., Al-Maagbeh, M. M., & Khalaileh, L. (2024). Artificial intelligence and its impact on administrative decision-making. *Journal of Human Security*. <https://doi.org/10.12924/johs2024.20114>
- Awaisheh, S. M., Alsaraireh, N., Alkasasbeh, A. A. M., & Odeibat, M. A. (2025). The extent to which recourse to arbitration is permissible in the settlement of procurement contract disputes. *Journal of Human Security*. <https://doi.org/10.12924/johs2025.210103>
- Awaisheh, S. M., Awaisheh, S. M., Abdelrahman, A., & Al-Thnaibat, O. H. A. (2025). Environmental governance and administrative judiciary in Jordan and France: A socio-legal comparative study. *International Journal*

- of *Sustainable Development and Planning*, 20(12), 5491–5501. <https://doi.org/10.18280/ijstdp.201238>
- Awaishah, S. M., Odeibat, M. A., Awaishah, S. M., Al Atiyat, M., Abdelrahman, A., & Al-Dabbas, N. A. (2026). Regulating commerce in the metaverse: Legal challenges of sales contracts in virtual environments [Special issue]. *Corporate Law & Governance Review*, 8(3), 214–222. <https://doi.org/10.22495/clgrv8i3sip3>
- Darawsheh, S. (2018). Civil liability of electronic signature certification authorities: A comparative analytical study. *Jerash Journal for Research and Studies*, 19(1).
- Dawwas, R. N. T. (2010). *Civil liability of the indirect tortfeasor: A comparative study* [Unpublished master's thesis]. An-Najah National University.
- European Union. (1999). *Directive 1999/93/EC on a Community framework for electronic signatures*. Official Journal of the European Communities.
- Haj Ali, A. A. M. (2013). *The legal regulation of electronic signature certification authorities* [Unpublished master's thesis]. An-Najah National University.
- Hashemite Kingdom of Jordan. (1976). Civil Code No. 43 of 1976 and its amendments. *Official Gazette*.
- Hashemite Kingdom of Jordan. (2014). Regulation No. 11 of 2014 on the licensing and accreditation of electronic authentication authorities and its amendments. *Official Gazette*, 5264.
- Hashemite Kingdom of Jordan. (2015). Electronic Transactions Law No. 15 of 2015. *Official Gazette*, 5341.
- Hijazi, A. B. (2007). *The legal framework of electronic signatures: A comparative study*. Dar Al-Kutub Al-Qanuniyah.
- Mohammed, B. A. S. (2020). *Contractual liability of online service providers: A comparative study* [Unpublished master's thesis]. Middle East University.
- Naseir, M. H. A., Al-Ali, E., Bqoor, K. J., Al-Wreikat, E. I., Al-Awaysheh, S. M., Awaishah, S. M., & Al-Khraisat, W. M. M. (2026). Shortcomings in medical civil liability in Jordan and the role of public administration in addressing them. *Genetics and Molecular Research*, 25(4s). <https://doi.org/10.4238/5psp6j89>
- Nasri, S. (2021). The nature of the liability of the electronic authentication authority. *Al-Manara Journal for Legal and Administrative Studies*, 35.
- Pérez Carrillo, E. F., & Alhasan, T. K. (2026). Building legally robust FIDIC 2017 e-claim infrastructures: Contract data design, platform governance, and enforcement of time bars. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, 18(4), Article 03726007. <https://doi.org/10.1061/JLADAH.LADR-1616>
- Rukba, R. O. A., Awaishah, S. M. A., Al-Hobabseh, W. I., Al-Khalaileh, L., Hmaidan, R. M., Althunibat, A. O., Awaishah, S. M., & Abdelrahman, A. (2025). Balancing efficiency and ethics in public administration: The role of artificial intelligence in administrative law of the Middle East. *Research Journal in Advanced Humanities*, 6(4). <https://doi.org/10.58256/ktbmht44>
- Tawakkul, F. M. A. (2010). *Electronic commerce contract*. Al-Halabi Legal Publications.
- Telecommunications Regulatory Commission. (2015). *Instructions for granting licenses or accreditation to electronic authentication authorities*. Hashemite Kingdom of Jordan.
- United Nations. (2001). *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*. United Nations.
- Yas, H., AlLouzi, A. S., Sarhan, M. I., Abdelrahman, A., Abdalaziz, M. M. O., & Al Banna, M. (2026). Social media platform accountability: How UAE law addresses misleading content and platform responsibility. *Acta Innovations*, 61, 747–757. <https://doi.org/10.62441/actainnovations.vi.842>