Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol.15, No.4, 2025, pp.302-308

DOI: https://doi.org/10.51983/ijiss-2025.IJISS.15.4.34

Safeguarding Electronic Signatures in Jordan: Legal Foundations and Enforcement Challenges

Khalid Abdulrahman Alhrerat[1*], Tariq Mohammad Qasim Alnsour[2], Saif Ibrahim Mohammad Almasarweh[3], Ammar Mohammad-Ali Alqudah[4], Dr. Salah Mohammed Aboudi Awaisheh[5] and Sadam Mohammad Awaisheh[6]

[1*]Associate Professor, Criminal Law, Faculty of Law, Al-Ahliyya Amman University, Amman, Jordan
[2]Assistant Professor, Common Law, Faculty of Law, Al-Ahliyya Amman University, Amman, Jordan
[3] Professor, Criminal Law, Faculty of Law, Mutah University, Jordan
[4]Civil Laws, Department of Special Law, Factually of Law, Al-Ahliyyah Amman University, Amman, Jordan
[5]Awaishesh Law Firm, Amman, Jordan
[6]Public Law Department, Faculty of Law, Al-Ahliyya Amman University, Jordan

E-mail: [1]k.alhrerat@ammanu.edu.jo, [2]t.alnsour@ammanu.edu.jo, [3]masarweh@mutah.edu.jo, [4]a.alqudah@ammanu.edu.jo, [5]salahalamda@yahoo.com, [6]s.awaisheh@ammanu.edu.jo
ORCID: [1]https://orcid.org/0000-0001-8355-8779,[2] https://orcid.org/0009-0002-6433-9735, [3]https://orcid.org/0009-0006-0769-6380, [4]https:orcid.org/0009-0000-8092-9001, [5]https://orcid.org/0009-0000-0800-4231, [6]https://orcid.org/:0000-0003-1984-8530

(Received 29 August 2025; Revised 15 October 2025, Accepted 03 November 2025; Available online 15 December 2025)

Abstract - This study examines Jordan's legal framework for protecting electronic signatures, focusing on the Electronic Transactions Law No. 29 of 2015 and the Cybercrimes Law No. 17 of 2023. The Electronic Transactions Law establishes technological neutrality by defining electronic signatures as data affixed to digital records and criminalizes fraudulent certificate creation and unauthorized disclosure of signatory secrets. The Cybercrimes Law complements these provisions by treating electronic signatures as part of broader "data," thereby criminalizing hostile interference -such as malware insertion, data theft, and unauthorized use- targeting signature-related information. Comparative insights from the UAE and Indonesia highlight common challenges in balancing security, enforcement capacity, and public awareness. Key enforcement gaps include under-resourced digital-forensics infrastructure, undefined criteria for "specialized judges," and low public understanding of certification requirements. The paper recommends statutory amendments to explicitly reference electronic signatures in the Cybercrimes Law, enhanced forensic and judicial training programs, and targeted public-awareness campaigns. By aligning intent thresholds, scaling penalties, and improving implementation capacity, Jordan can ensure that its legal regime sustains trust, identity verification, and transactional security in e-commerce.

Keywords: Electronic Signature Protection, Jordan E‑Commerce Law, Cybercrimes Law, Digital Forensics, Certification Authorities, Public Awareness

I. INTRODUCTION

E-commerce now contributes nearly 15 percent of Jordan's retail activity, pressuring legislators to endow digital transactions with the same juridical force as ink-on-paper deals (Al-Masadeh et al., 2024). Two statutes anchor this policy: the Electronic Transactions Law No. 29 of 2015 ("ET Law"), which confers full evidentiary status on electronic documents and signatures through a Certification-Authority ("CA") licensing regime, and the Cybercrimes Law No. 17 of 2023 ("CL 2023"), whose data-centric offences implicitly extend criminal protection to signature-creation and verification data (Barak, 2024). Together they promise technological neutrality, consumer-oriented cyber-security, and deterrence against forgery, malware, and illicit key-exfiltration. Yet Jordan's dual-statute architecture has not been stress-tested in practice. First, the ET Law's offences target fraudulent certificate issuance and insider disclosures but leave post-issuance threats such as stealthy key-theft to the more recent CL 2023. Second, CL 2023 does not define "electronic signature" expressly, creating interpretive uncertainty about mens-rea thresholds and charge selection (Ha, 2024). Third, under-resourced digital-forensics labs, undefined criteria for "specialised judges," and limited public awareness of CA requirements blunt the statutes' deterrent potential (Al-Freihat et al., 2024; Hjort et al., 2025). No published study has yet synthesised these doctrinal overlaps or benchmarked Jordan's enforcement performance against regional peers. This article fills that lacuna through doctrinal analysis. It addresses four research questions: (1) Do overlapping offences generate doctrinal redundancy or prosecutorial gaps? (2) Does the absence of explicit signature language in CL 2023 hinder convictions? (3) How do Jordan's mens-rea and sanction regimes compare with those of the UAE and Indonesia selected for their contrasting tiered-security and turnover-based models? (4) What institutional reforms would best fortify Jordan's digital-signature ecosystem? (Chauhan & Bhatia, 2025). The paper proceeds in five parts: statutory mapping, doctrinal critique,

comparative evaluation, enforcement diagnostics, and reform proposals. By aligning mental-state thresholds, scaling penalties to organisational size, and bolstering digital-forensics capacity, Jordan can transform its promising legislative edifice into a regional benchmark for secure, trust-based digital trade.

II. CONCEPTUAL FOUNDATIONS

2.1 Statutory Definition of "Electronic Signature"

Article 2 of Jordan's Electronic Transactions Law No. 29 of 2015 (hereafter "ET Law") defines an electronic signature as "data that take the form of letters, numbers, symbols, signs, or other elements" affixed to or logically associated with an electronic record for the purpose of identifying the signatory and preventing unauthorised use (ET Law, 2015, art. 2). By legislatively equating this digital marker with a handwritten signature, Parliament resolved a doctrinal uncertainty that had long hampered enforceability in cyberspace. The breadth of the definition embracing both embedded and linked data ensures technological neutrality, allowing the rule to accommodate evolving authentication tools without statutory amendment. Yet the very openness of the clause raises interpretive questions about minimum reliability thresholds and certification standards issues that remain under-explored in Jordanian scholarship (Awaisheh, 2025).

2.2 Protected Interests: Trust, Identity Verification, and Transaction Security

Safeguarding electronic signatures serves three interlocking interests. Trust is foundational: users must believe that a digital mark genuinely emanates from the purported signatory (Haikal et al., 2024). Without this assurance, e-commerce reverts to paper or collapses into costly interpersonal verification. Identity verification is the doctrinal mechanism that transforms trust into legal certainty; Certification Authorities (CAs) perform a gatekeeping role, binding a cryptographic key pair to a natural or juristic person (Alhasan, 2025a). Finally, transaction security the guarantee that messages are intact and non-repudiable protects both parties' reliance interests and undergirds speedy, automated performance (Khater, 2024).

These interests operate cumulatively. Where identity is ambiguous, trust erodes; when either element falters, security deteriorates, inviting fraud and deterring commercial uptake (Abu Issa et al., 2019; Al-Billeh et al., 2024).

III. CRIMINAL SAFEGUARDS UNDER THE ELECTRONIC TRANSACTIONS LAW

3.1 Structure of Offences: Formal versus Material

Jordanian criminal doctrine distinguishes material offences where harm to a legally protected interest must eventuate from formal (or "danger") offences, completed the moment the proscribed conduct occurs, irrespective of damage (Al-Saʿīd, 2022). Sections 24 and 25 of the ET Law adopt the latter model: both target conduct that imperils the authenticity or confidentiality of electronic signatures without requiring proof of downstream loss. This preventive framing tracks the legislature's policy objective: maintaining ex ante confidence in e-transactions by deterring manipulations that could erode verification and non-repudiation (Awaisheh, 2023). The choice of misdemeanour penalties imprisonment or substantial fines signals proportionality: high enough to discourage wrongdoing yet calibrated below felony thresholds so as not to chill legitimate digital activity (Al-Khalaileh et al., 2025).

3.2 Offence 1 – Creation, Publication, or Presentation of Fraudulent Authentication Certificates (ET Law, s 24)

Actus reus. Section 24 criminalises three alternative actions: creation (generating a certificate ex nihilo), publication (disseminating it indiscriminately), and presentation (deploying it for advantage). Each act is self-executing; the offence is consummated once any single limb is completed, even if no contract is actually induced (Al-Majali, 2022).

Mens rea. The provision demands specific intent: knowledge of the falsity of the certificate and a fraudulent purpose. Mere negligence in vetting a certificate would therefore fall outside the ambit of s 24, though ancillary liability (e.g., aiding and abetting) may still arise under the Penal Code (Issa & Alkhseilat, 2022).

Penalty. The legislature prescribes imprisonment of three months to three years or a fine between JOD 10,000 and JOD 50,000; cumulatively, where warranted. The broad sentencing band affords courts discretion to calibrate punishment to gravity e.g., a short custodial term for isolated misconduct versus a maximum fine for systematic "certificate factories."

Doctrinal assessment. By classifying the offence as formal, Parliament shifts evidentiary focus from proving end-user deception to verifying falsification at source, easing prosecutorial burdens and aligning with international best practice under UNCITRAL Model Law art. 17 (Awaisheh, 2023; Alhasan, 2025b). However, clarification is still needed on whether partial falsification such as manipulating expiry dates suffices for liability.

3.3 Offence 2 – Disclosure of Signatory Secrets by Certification Authorities (ET Law, s 25)

Actus reus. The core conduct is "disclosure," expansively defined to include oral, written, visual, or electronic revelation of any data capable of identifying the signatory's private key or related credentials (Al-Manaʿiṣah & Al-Zuʿbi, 2017). Because confidentiality is breached at the moment of unauthorised access, the provision again operates as a formal offence (Nasīmah, 2020).

Mens rea. Intentionality is required; inadvertent system leaks are excluded but may ground administrative liability under CA licensing regulations (Abu Issa et al., 2019). The statute is silent on recklessness. Doctrinal lacuna commentators suggest closing to address grossly negligent data-security lapses (Khater, 2024).

Corporate liability. Certification Authorities are almost invariably juristic persons. Section 25 therefore imposes a primary fine of JOD 50,000–100,000 and empowers regulators to revoke licences. This strict-yet-monetary sanction reflects comparative practice in the EU eIDAS Regulation, which likewise favours pecuniary and supervisory measures over incarceration for corporate offenders (Alshible & Abu Issa, 2025).

Doctrinal assessment. Section 25 operationalises the principle of data fiduciary duty: CAs occupy a position of asymmetric knowledge and must protect subscriber secrets. Yet the section's focus on disclosure leaves ambiguous whether negligent retention of outdated keys, which could expose users to spoofing, is covered. Commentary proposes a supplementary duty of "secure deletion" to close this loophole (Edisherashvili, 2020).

IV. Criminal Safeguards under the Cybercrimes Law 2023

4.1 Doctrinal Inclusion of the Electronic Signature as "Data"

Although Cybercrimes Law No. 17 of 2023 ("Cybercrimes Law") does not explicitly invoke the term "electronic signature," its definition of "data" is sufficiently capacious to encompass any digital artefact that meets the statutory contours of an electronic signature (Edisherashvili, 2020). Article 2 of the Electronic Transactions Law No 29 of 2015 ("ET Law") characterises an electronic signature as "data that take the form of letters, numbers, symbols, signs, or other elements, which are recorded electronically or by any similar means in the electronic ledger, or are added to or linked with it for the purpose of identifying the signatory and ensuring that no one else may use it." By importing this definition into a broader cyber-offences regime where "data" is the primary object of protection the legislature effectively extends Cybercrimes Law sanctions to any assault on information intrinsically constituting an electronic signature (Awaisheh, 2023).

Doctrinally, this approach reflects a functionalist logic: an electronic signature is not treated as a sui generis legal construct but rather as a subset of "electronic content" covered by the Cybercrimes Law. Consequently, offences designed to protect "data" under Articles 6–9 automatically safeguard the integrity, confidentiality, and availability of electronic signatures, even in the absence of express textual reference. However, this inclusive framing may give rise to interpretive challenges most notably, whether a purely descriptive dataset (e.g., metadata used in e-authentication) qualifies as "data" under the Cybercrimes Law's scope, and whether the ET Law's reliability and non-repudiation requirements carry over in full doctrinal force (Khater, 2024). These ambiguities warrant scholarly attention, as they bear on prosecutorial thresholds and judicial interpretation in digital-evidence adjudication.

4.2 Offence Group A – Assault on the Signature Data (s 6)

Actus reus. Under Article 6, the Cybercrimes Law criminalises any act that "inserts, publishes, [or] uses a program or software command via the information network or IT means [that] destroys electronic content." Because an electronic signature is by definition "data recorded electronically" (ET Law, 2015, art. 2), any deployment of malicious code viruses, worms, Trojan horses, logic bombs targeting systems that store or process electronic signature data falls squarely within the statutorily proscribed actus reus (Barak, 2024). This offence is formal in nature: injurious consequences (such as actual deletion or corruption) are not required.

could evade prosecution under this provision (Awaisheh, 2025). Comparative statutes, such as Article 3 of the EU NIS 2 Directive, distinguish between data theft and data sabotage; Jordanian law might benefit from a similar bifurcation.

4.3 Offence Group B – Payment-Method–Related Misdemeanours (s 8)

4.3.1 Misdemeanour of Obtaining Electronic Signature Data for Electronic Payment Methods Actus reus

Mens rea. Proof of criminal intent requires two elements: (1) knowledge that the data being acquired consist of someone else's electronic signature credentials, and (2) a will to seize those credentials without the owner's permission. Mere recklessness e.g., deploying a generic phishing scheme without specific knowledge that a private key would be captured may be insufficient to satisfy this stringent mens rea requirement (Alghuwairi et al., 2024).

4.3.2 Misdemeanour of Accepting to Transact with Illicitly Obtained Electronic Payment Data

Actus reus. Also under Article 8, paragraph A/3, the law penalises those who "accept to transact with electronic signature data for payment" when they have knowledge that such data were obtained unlawfully. The criminal conduct is realized passively: refraining from refusal once illegal data is offered for a transaction suffices (Al-Billeh et al., 2024).

Mens rea. Only general intent is required: the actor must know that the data were illicitly obtained but need not harbour a specific objective beyond accepting them (Al-Saeed, 2022). Thus, a merchant who knowingly processes an online payment with stolen e-signature credentials triggers liability, even if her intent was only to earn legitimate revenue (Al-Khazraji, 2022).

Penalty. Imprisonment ranges from one to three years, and the fine is JOD 2,500–10,000. If the illicit data is used to

withdraw or benefit from another's funds, the penalty escalates to imprisonment of two to three years and a fine of JOD 5,000–15,000. Should actual monetary seizure occur, the maximum rises to three years and a fine of JOD 10,000–20,000, even if no actual loss has yet materialised.

Doctrinal notes. By criminalising passive acceptance, the legislature aimed to stem the market for stolen e-signature credentials. Yet the broad scope of "acceptance" may ensnare intermediaries with only tenuous knowledge such as payment-gateway operators leading to potential over-criminalisation absent clear safe-harbour provisions (Issa & Alkhseilat, 2022).

4.4 Offence Group C – Felony Assault on Banking-Service Data (s 9)

Aggravating factors (s 27). Article 27(2) doubles penalties if the offence is committed "through exploitation of one's position, work, or authority," "for the benefit of a foreign state or illegitimate organisation," "against multiple victims," or "as a recidivist." However, the statute does not specify objective criteria such as a minimum victim count or recurring-offender thresholds leaving these determinations to judicial discretion (Al-Freihat et al., 2024; Biswakarma, 2014).

Reducing penalties for self-disclosure (s 29). To encourage co-operation from those involved in complex cybercrimes, Article 29 grants courts discretion to reduce penalties by half if an offender voluntarily discloses the offence before detection. This measure reflects a restorative justice impulse aimed at unravelling multi-actor schemes and addressing evidentiary challenges inherent in cyber investigations (Nazran et al., 2024).

4.5 Procedural & Evidentiary Provisions (s 31–36)

Precautionary measures (s 31). Article 31 empowers courts to order confiscation of devices used in the crime, disable compromised information systems or websites, and close premises from which offences emanated. By pairing substantive sanctions with dispositive injunctions, the legislature seeks to neutralise ongoing threats without prejudice to third parties acting in good faith. This mirrors international best practice under the Budapest Convention, which endorses immediate preservation of digital evidence (Jacobs, 2024; Awaisheh et al., 2024).

Urgency and specialised competence (s 34–35). To expedite adjudication, Article 34 mandates that cyber-offence cases be heard at least weekly and resolved within three months of registration. Article 35 requires "specialised judges" for investigation and trial, reflecting recognition that technical complexity demands dedicated expertise. Absent statutory criteria for "specialisation," however, the composition of such benches may vary across jurisdictions, possibly undermining consistency (Qu et al., 2025).

Digital-evidence valuation (s 36). Within a predominantly free-evidence regime derived from the Latin tradition, Article 36 expressly confers probative value upon digital evidence whether originating domestically or abroad and deems the protocol header (i.e., metadata marking timestamp and transmission nodes) a valid proof source. The provision further criminalises concealment, tampering, or destruction of digital evidence, punishable by at least three months' imprisonment (Comande & Varilek, 2024). By codifying the protocol header's evidentiary status, Parliament addresses a doctrinal lacuna, ensuring that courts may rely on metadata even if opposing parties contest its admissibility (Nasīmah, 2020).

Doctrinal assessment. These procedural measures collectively aim to accelerate justice and bolster confidence in digital forensics. Still, "specialised judges" raises questions about credentialing must they hold ICT certifications, or simply have practical experience? Codifying minimal qualification thresholds (e.g., mandated training modules) would reduce arbitrariness (Hjort et al., 2025). Furthermore, while privileging the protocol header aligns with comparative practice in the EU's e-Evidence Regulation, it may also invite debates over chain-of-custody integrity when evidence crosses jurisdictional borders (Issayeva et al., 2024).

V. CROSS-REGIME SYNTHESIS AND POLICY EVALUATION

Jordan's two primary statutes the Electronic Transactions Law No. 29 of 2015 (ET Law) and the Cybercrimes Law No. 17 of 2023 (CL 2023) operate in tandem to protect electronic signatures, yet they differ substantially in scope, mens rea thresholds, and sanction severity. While the ET Law focuses on insider and certificate-authority misconduct (specifically, fraudulent certificate creation and unauthorized disclosure of signatory secrets), the CL 2023 casts a broader net by criminalizing virtually any hostile interference with digital "data," thereby encompassing electronic signatures within a more expansive cyber-offences framework (Alhassan, 2025b; Barak, 2024).

5.1 Deterrent Reach

Under the ET Law, criminal liability attaches primarily to actors directly connected with Certification Authorities (CAs) or those fabricating or disclosing false certificates (Electronic Transactions Law, 2015, §§ 24–25). By contrast, CL 2023 extends liability to any individual who "inserts, publishes, or uses a program or software command" to destroy or alter electronic content, including e-signature data (Cybercrimes Law, 2023, art. 6). Similarly, CL 2023's Article 8 criminalizes "obtaining data that may comprise the electronic signature" for payment fraud and "accepting to transact with electronic signature data" knowing it was unlawfully procured (Cybercrimes Law, 2023, art. 8). Consequently, CL 2023's offences capture external cyberattackers hackers, malware distributors, and illicit data

brokers that ET Law's more circumscribed clauses would miss (Comandè & Varilek, 2024; Khater, 2024).

This wider reach aligns with international best practices, which recognize the need to safeguard digital-asset integrity beyond certificate issuance (European Union, 2014). However, the ET Law's narrower focus may leave post-issuance threats such as exfiltration of private-key data governed only by CL 2023, potentially creating gaps if prosecutors misapply the wrong statute (Awaisheh, 2025).

In contrast, the CL 2023 sets mixed mens rea standards. Article 6 (assaulting e-signature data via malware) insists on specific intent to "cancel, destroy, delete, or assault" data (Cybercrimes Law, 2023, art. 6). By making it a formal offence, courts need not wait for actual damage to occur (Barak, 2024). However, Article 8(3) (accepting illicit payment data) only requires general intent or "knowledge" that the data were unlawfully obtained (Cybercrimes Law, 2023, art. 8(3)). Finally, Article 9 (felony assault on banking-service data) presumes the perpetrator's knowledge that targeted data pertain to money transfers or payment services, with general intent sufficing (Cybercrimes Law, 2023, art. 9; Al-Majali, 2022).

5.3 Sanction Severity

Under the ET Law, Sections 24 and 25 classify both fraudulent certificate creation and unauthorized disclosure as misdemeanours punishable by imprisonment of three months to three years or fines of JOD 10,000–50,000 (Electronic Transactions Law, 2015, §§ 24–25). In practice, the ET Law's maximum fine (JOD 50,000) may be an inadequate deterrent for large multinational CAs with annual turnover far exceeding that amount; by contrast, the EU's eIDAS Regulation allows fines up to 3% of global turnover for trust-service providers (European Union, 2014).

Conversely, CL 2023 differentiates misdemeanours and felonies more sharply. Article 6's malware assault is a misdemeanour punishable by six months to three years' imprisonment and fines of JOD 2,500–10,000 (Cybercrimes Law, 2023, art. 6). Article 8(1) (obtaining signature data) also carries one to three years of imprisonment and fines of JOD 2,500–10,000 (Cybercrimes Law, 2023, art. 8(1)); Article 8(3) (accepting illicit data) ranges likewise but increases to two to three years' imprisonment and JOD 5,000–15,000 fines if used to seize funds, and to three years plus JOD 10,000–20,000 if loss actually occurs (Cybercrimes Law, 2023, art. 8(3)). By contrast, Article 9's felony assault on banking-service data is severe: temporary hard labour for a minimum of five years and fines of JOD 25,000–75,000 (Cybercrimes Law, 2023, art. 9) (Agbeja & Afolabi, 2016). These enhanced sanctions reflect legislators' recognition of the systemic threat posed by attacks on financial infrastructure (Al-Majali, 2022; Bensafi & Usun 2023).

Thus, CL 2023's graduated penalties exceed those in the ET Law for comparable digital-asset misconduct. The stark contrast e.g., JOD 75,000 fine plus hard labour for a felony versus JOD 50,000 maximum fine for ET Law misdemeanours may incentivize prosecutors to prefer CL 2023 when evidence supports banking-service data jurisdiction (Jamithireddy, 2025). However, if courts misapply CL 2023 to CA insider wrongdoing (better suited to ET Law), either over- or under-punishment could occur, undermining doctrinal coherence (Alshible & Abu Issa, 2025; Barak, 2024).

5.5 Policy Considerations

To address these deficits, the following policy measures merit consideration:

1. **Harmonize Mens Rea Standards.** Amend ET Law § 25 to include recklessness or gross negligence as an alternative mental state for unauthorized disclosure by CAs. This would mirror CL 2023's mixed-intent approach, ensuring that inadvertent but high-risk CA misconfigurations do not slip outside criminal purview (Al-Billeh et al., 2024; Aawishe et al., 2024).
2. **Adopt Scalable Penalties.** Introduce turnover-based fines for CAs under ET Law § 25, akin to the EU's eIDAS model, ensuring sanctions scale with organizational size and global revenue (Salemink et al., 2024; Ha, 2024). Similarly, CL 2023 misdemeanour fines could be tiered based on the volume of data exfiltrated or financial loss prevented.
3. **Clarify Dual-Charging Guidelines.** Publish prosecutorial guidance delineating which statute ET Law or CL 2023 applies to various permutations of e-signature misconduct. Clear criteria (e.g., whether the initial breach occurred at a CA or via external intrusion) would reduce prosecutorial discretion and sentencing unpredictability (Al-Rai & AlOmran, 2024).
4. **Upgrade Forensic Capacity.** Invest in public digital-forensics laboratories, train personnel in advanced malware analysis, and foster partnerships with academia for joint research. Establish Memoranda of Understanding (MOUs) with international 24/7 network partners under the Budapest Convention to expedite evidence sharing (Al Masadeh et al., 2024).
5. **Bolster Judicial Training.** Define "specialised judges" via statutory amendments or judicial council directives, mandating ICT certification or periodic cybercrime continuing legal education (CLE) credits (Şenol et al., 2024). Creating a central cybercrime bench with standard operating procedures would promote uniform interpretive approaches (Albalawee, 2024).
6. **Enhance Public Awareness Campaigns.** Collaborate with the Central Bank of Jordan and JoPACC (Jordanian Public-Private Accreditation Council) to conduct nation-wide e-signature literacy programs targeting SMEs, artisans, and university students. Emphasize criminal risks of uncertified e-

signature usage and the penalties under both statutes (Al-Rai & AlOmran, 2024; Al Amad et al., 2024).

VI. Comparative Snapshot: UAE and Indonesia

Jordan's legal architecture for electronic signatures and related criminal protections reflects a broader global recognition of the need to safeguard trust in digital commerce. A brief comparison with the United Arab Emirates (UAE) and Indonesia underscores shared challenges such as balancing technological neutrality with robust security and situates Jordan's regime relative to two jurisdictions that have also enacted comprehensive electronic-transaction statutes.

In the UAE, the Federal Decree-Law No. (46) of 2021 on Electronic Transactions and Trust Services establishes a framework that not only recognizes the legal validity of electronic signatures but also criminalizes malicious interference with signature-creation data. Article 47 of the UAE Decree-Law stipulates that "imposition of the penalties stipulated in this Decree Law shall not prejudice any more severe penalty stipulated in any other law" (Federal Decree-Law No. 46/2021, 2021, art. 47). This broad language essentially ensures that criminal sanctions for electronic-signature forgery or unauthorized disclosure can be compounded by more severe penalties under other statutes. Moreover, the UAE law defines distinct security levels and prescribes that qualified trust service providers must "protect the Electronic Signature Creation Data against any use by third parties or forgery using the available technology" (Federal Decree-Law No. 46/2021, 2021, art. 18). By contrast, Jordan's Electronic Transactions Law No. 29 of 2015 criminalizes certificate-related misconduct primarily through formal (danger) offences such as creating fraudulent payment certificates (ET Law, 2015, § 24) and places relatively lower maximum fines (JOD 50,000) compared to the UAE's tiered security-level approach (Al Masadeh et al., 2024; Federal Decree-Law No. 46/2021, 2021, arts. 18, 47). Thus, while Jordan's statutory design emphasizes preventive formal offences, the UAE's regime integrates a graduated security-classification scheme, potentially offering more nuanced deterrence calibrated to transaction risk (Alsheyab, 2023; Federal Decree-Law No. 46/2021, 2021).

Indonesia's Information and Electronic Transactions Law (the "EIT Law"), initially enacted as Law No. 11 of 2008, has undergone multiple amendments in 2016 and 2024 to strengthen criminal sanctions for electronic fraud and signature abuse (Al Masadeh et al., 2024). Under the second amendment (Law No. 1 of 2024), high-risk electronic transactions especially financial transactions not conducted face-to-face must be executed with electronic signatures secured by certified electronic certificates (Sovrano et al., 2024). Notably, Article 27B (1) explicitly criminalizes "the public dissemination of electronic information/documents aimed at unlawful self-benefit," which encompasses forging or altering signature data (Proposed EIT Law Amendments, 2024). Penalties for digital-signature–related crimes in Indonesia now include prison terms of up to six years for aggravated offences such as fraudulent fund transfers, and fines scaled by the severity of inflicted losses (Şenol et al., 2024). In comparison, Jordan's Cybercrimes Law No. 17 of 2023 designates felony assault on banking-service data including signature data related to money transfers as punishable by a minimum of five years' hard labour and fines up to JOD 75,000 (Cybercrimes Law, 2023, art. 9; Laghareh et al., 2018). While both Indonesia and Jordan prescribe severe sanctions for financial-data breaches, Indonesia's turnover-based or loss-scaled fines (e.g., fines up to 3 billion IDR for major breaches) reflect a more dynamic scaling mechanism than Jordan's flat bracket (Cybercrimes Law, 2023, art. 9).

All three jurisdictions grapple with similar enforcement obstacles most notably, under-resourced digital forensics labs, uneven judicial technical capacity, and public awareness gaps (Al Masadeh et al., 2024). The UAE has sought to address these by establishing accredited trust-service testing bodies (Al-Rai & AlOmran, 2024; Alhasan & Burr, 2025), while Indonesia has launched nationwide e-signature literacy campaigns and bolstered cybercrime units within the police (Abu Issa et al., 2019; Awaisheh, 2023).

In sum, although Jordan's ET Law and Cybercrimes Law provide substantive criminal safeguards comparable to those in the UAE and Indonesia, Jordan's regime remains less granular in differentiating risk levels and scaling sanctions, and its enforcement capacity is still evolving. Nevertheless, the shared acknowledgement across these jurisdictions that robust criminal protections are essential to sustain trust, identity verification, and security in electronic dealings highlights a global consensus and validates Jordan's approach as broadly aligned with international trends, even as each state tailors its statutes to domestic priorities and resource constraints.

In summary, Jordan's commitment to frictionless, trustworthy electronic commerce remains evident in its legislative architecture. Yet realizing these ambitions in practice requires closing doctrinal gaps, bolstering enforcement capacity, and elevating public awareness. By clarifying statutory references to electronic signatures in the Cybercrimes Law and strengthening the supporting infrastructure and education mechanisms, Jordan can ensure that its legal framework fulfills the dual goals of speed and certainty in electronic dealings. Continued attention to these reforms will be critical as e-commerce evolves and cyberthreats become more sophisticated, ensuring that digital transactions remain both efficient and secure.

References

[1] Aawishe, 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

[2] Agbeja, O., & Afolabi, C. (2016). Cash Management Effect on Corporate Going-Concern Status: A Comparative Study of Manufacturing Companies and Deposit Money Banks in Ghana and

Nigeria (2010-2014). *International Academic Journal of Social Sciences, 3*(2), 82–95.

[3] Al Amad, M., Alzobi, A., Abo Taleb, R., & Al Hanini, E. (2024). The impact of expert systems on limiting electronic fraud in Jordanian commercial banks. *Al-Balqa Journal for Research and Studies, 27*(4), 56–78. https://doi.org/10.35875/77mj0e76

[4] Al Masadeh, A. M., Abunaseir, M. H., & Rukba, R. O. A. (2024). Impact of Jordanian Electronic Transactions Law and Digital Transformation on Commercial Contracts and Their Proof. *Journal of Human Security*, *20*(1), 104-108.

[5] Albalawee, N. (2024). E-Contracting within Jordan's Legal Framework. *Pakistan Journal of Criminology*, *16*(1). https://doi.org/10.62271/pjc.16.1.331.343

[6] Al-Freihat, M., Al-Hussien, S., Balas, H., Al-Sarayrah, A., Al-Smadi, M., Aleissa, T., & Al-Wahshat, Z. (2024). Electronic commerce contracts under Jordanian law: A legal perspective. *Malaysian J. Syariah & L.*, *12*, 447. https://doi.org/10.33102/mjsl.vol12no2.565

[7] Alghuwairi, A., AL-Khalaileh, L., Al-Billeh, T., Al-Qheiw, M. A., & Almamari, A. (2024). Penal Protection for the Consumer in E-Commerce Contracts by the Provisions of Jordanian Legislation. *Pakistan Journal of Criminology*, *16*(2). Bensafi, A.-E.-H., & Usun, S. (2023). Explainable AI models in financial risk prediction: Bridging accuracy and interpretability in modern finance. *Electronics, Communications, and Computing Summit, 1*(1), 67–75.

[8] Alhasan, T. K. (2025). Integrating AI into arbitration: Balancing efficiency with fairness and legal compliance. *Conflict Resolution Quarterly*. https://doi.org/10.1002/crq.21470

[9] Al-Khazraji, O. (2022). General section of the Penal Code (1st ed.). Dar Al-Badeel for Publishing and Distribution.

[10] Al-Majali, N. (2022). *Explanation of the Penal Code, General Section: An analytical study in the general theory of crime and criminal liability.* Dar Al-Thaqafa for Publishing and Distribution.

[11] Al-Rai, A. F., & AlOmran, N. M. (2024). Criminal protection of electronic signatures from forgery in Jordanian and UAE legislation. *International Journal of Electronic Governance*, *16*(2), 246-262. https://doi.org/10.1504/IJEG.2024.140786

[12] Al-Saeed, K. (2022). *Explanation of the general provisions in the penal code: A comparative study* (5th ed.). Dar Al.

[13] Alsheyab, M. S. A. (2023). Legal recognition of electronic signature in commercial transactions: A comparison between the Jordanian electronic transaction's law of 2015 and the United Arab Emirates electronic transactions and trust services law of 2021. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, *36*(3), 1281-1291. https://doi.org/10.1007/s11196-022-09967-6

[14] Alshible, M., & Issa, H. A. (2025). Criminal protection to the digital right to be forgotten in Jordan. *International Journal of Electronic Security and Digital Forensics*, *17*(3), 295-306. https://doi.org/10.1504/IJESDF.2025.145865

[15] Awaisheh, S. M. (2023). Digital justice in Jordan: the role of virtual arbitration sessions in modernizing the legal system. *International Journal of Cyber Criminology*, *17*(1), 146-165.

[16] Awaisheh, S. M. (2025). From paper to pixels: the legal status and challenges of electronic writing in administrative contracts. A comparative study of current legal systems. *Electronic Government, an International Journal*, *21*(2), 210-226. https://doi.org/10.1504/EG.2025.144726

[17] Awaisheh, S. M., Alkhamaiseh, M. A., AL-Maagbeh, M. M., Al Khalaileh, L., Khreisat, M. K., & AlAtiyat, M. (2024). Artificial intelligence and its impact on administrative decision-making. *Journal of Human Security*, *20*(1), 99-103.

[18] Barak, A. (2024). *Explanation of the Cybercrimes Law: Conceptual framework, substantive confrontation, procedural confrontation in light of Law No. 17 of 2023.* Dar al-Thaqāfah for Publishing and Distribution.

[19] Biswakarma, G. (2014). Organizational Career Growth and Employees‟ Turnover Intentions: An Empirical Evidence from Nepalese Private Commercial Banks. *International Academic Journal of Organizational Behavior and Human Resource Management, 1*(1), 1–17.

[20] Chauhan, P., & Bhatia, A. D. (2025). Digital Transformation in Public Sector ICT: A Case Study-Based Comparative Analysis. *International Academic Journal of Innovative Research*, *12*(3), 27-32. https://doi.org/10.71086/IAJIR/V12I3/IAJIR1222

[21] Comande, G., & Varilek, M. (2024). The many features which make the eIDAS 2 Digital Wallet either risky or the ideal vehicle for the transition to post-quantum encryption. *Computer Law & Security Review*, *54*, 106022. https://doi.org/10.1016/j.clsr.2024.106022

[22] Edisherashvili, T. (2020). Legal regalements of e-signature. *Journal of Legal Studies "Vasile Goldiş"*, *25*(39), 98-127.

[23] Ha, L. T. T. (2024). Interrelation between electronic signature laws in Malaysia and Vietnam in electronic transactions. *Pakistan Journal of Life and Social Sciences, 22*(2), 3200–3219. https://doi.org/10.57239/PJLSS-2024-22.2.00234

[24] Haikal, M. N., & Mahmudah, S. (2024). Implementation, advantages and barriers and legal protection against the use of electronic signatures. *Journal of Social Research*, *3*(6), 1179-1195. https://doi.org/10.55324/josr.v3i6.2067

[25] Hjort, M. A., Kalamees, P., & Kask, L. (2025). Misuse of Electronic Signatures and eID Owner Liability: A Comparative Analysis of Estonian and Norwegian Legislative Frameworks and Practice. *European Business Law Review*, *36*(2). https://doi.org/10.54648/eulr2025012

[26] Issa, H. A., & Alkhseilat, A. (2022). The cyber espionage crimes in the Jordanian law. *International Journal of Electronic Security and Digital Forensics*, *14*(2), 111-123. https://doi.org/10.1504/IJESDF.2022.121203

[27] Issayeva, A., Niyazbekova, S., Semenov, A., Kerimkhulle, S., & Sayimova, M. (2024). Digital Technologies and the Integration of a Green Economy: Legal Peculiarities and Electronic Transactions. *Reliability: Theory & Applications*, *19*(SI 6 (81)), 1088-1096. https://doi.org/10.24412/1932-2321-2024-681-1088-1096

[28] Jacobs, B. (2024). The authenticity crisis. *Computer Law & Security Review*, *53*, 105962. https://doi.org/10.1016/j.clsr.2024.105962

[29] Jamithireddy, N. S. (2025). Failure propagation in SAP MultiBank payment batches due to unsynchronized secure channel negotiations. *Journal of Information Systems and Information Security, 13*(2), Article 036. https://doi.org/10.58346/JISIS.2025.I2.036

[30] Khater, M. N. (2024). Criminalization of Forgery of Electronic Payment Cards in Jordanian Legislation. *Pakistan Journal of Criminology*, *16*(1). https://doi.org/10.62271/pjc.16.1.441.455

[31] Laghareh, F. S., Mirabedini, S. J., & Abadi, A. H. (2018). Provide a Method for Validation of Bank Customers Using Data Mining Techniques (Case Study: Bank Sepah). *International Academic Journal of Science and Engineering.* https://doi.org/10.9756/IAJSE/V5I1/1810032

[32] Nasīmah, T. (2020). Criminal protection of the electronic signature: A comparative study (Unpublished doctoral dissertation). Ibn Khaldūn University–Tiaret.

[33] Nazran, F., Purba, H., Saidin, O. K., & Kaban, M. (2024). Legal Protection of Notaries in Document Validation through Technology-Based Systems: A Comparative Legal Review of Indonesia, the United States, the Netherlands, and Australia. *Journal of Ecohumanism*, *3*(7), 4975-4982. https://doi.org/10.62754/joe.v3i7.4608

[34] Salemink, T., Wolters, P., & De Wulf, H. (2024). Cybersecurity and online formation of companies in the Netherlands, Belgium, and Germany. *European Company and Financial Law Review*, *21*(1), 67-103. https://doi.org/10.1515/ecfr-2024-0003

[35] Sovrano, F., Palmirani, M., Sapienza, S., & Pistone, V. (2024). DiscoLQA: zero-shot discourse-based legal question answering on European Legislation. *Artificial Intelligence and Law*, 1-37. https://doi.org/10.1007/s10506-023-09387-2