Customary Law Journal, ICLSSEE Special Collection 2026, *Page*: 1-9

Reconstructing The Role of Notaries in Electronic Commerce: A Notary-Based Digital Authentication Model for Ensuring Legal Certainty in Electronic Contracts

Andrian Danul Firmansyah*, Tina Amelia

Universitas Borobudur, Jakarta, Indonesia, andriandf@gmail.com

Universitas Borobudur, Jakarta, Indonesia, tinaamelia@borobudur.ac.id

DOI:
https://doi.org/10.47134/jcl.v3i3.1.5845
*Correspondence: Andrian Danul Firmansyah
Email: andriandf@gmail.com

Received: 26/05/2026
Accepted: 27/06/2026
Published: 27/06/2026

Abstract: *The digital transformation of commerce through electronic system (e-commecer) has fundamentally shifted the paradigm of contract law from physical interaction-based agreements to technology-driven transactions. Although electronic contracts have gained legal recognition, their practical implementation continues to face fundamental challenge, particulary in ensuring legal certainty, identity verivication, legal capacity, and the validity of consent, which is often reduce to a mere "click to agree" formality. These conditions reveal a structural gap between classical contract law principles and the realities of digital transactions. This study aims to critically examine the validity of electronic contracts under indonesian law and to reconstruct the role of notaries in ensuring legal certainty within digital transactions. The research employs a normative juridicial method combined with statutory, conceptual, and comparative approaches, analyzing legal frameworks in the Eropean Union, the United States, and Singapore. The finding indicate that te primary weakness lies in the absence of robust identity authentication mechanisms and the lack of reliable authority to verify the legal capacity of contracting parties. Therefore, this study proposes the Notary-Bases digital Authentication model (NDAM) as a alegal reconstruction framework that positions notaries as digital trust authorites. The model integrates digital identity verification, legal capacity assessment, contract authentication, and electronic signature validation within a unifies system.the main contribution of this research lies in the development of a normative model that bridges the structural gap between classical contract law and the digital ecosystem, thereby enhacing legal certainty and trust in electronic transactions.*

Keywords: *Electronic Contracts, Notary, Legal Certainty, E-Commerce, Digital Authentication*

Introduction

The rapid development of information technology has significantly transformed the structure of legal relation in modern society, particularly in the field of commerce, which is increasingly relies on electronic systems as the primary medium for conducting business transactions (Ramli, 2004). The emergence of Electronic Commerce has created a borderless transactional environment, where parties may encounter into legally binding agreements without physical interaction, thereby redefining traditional concepts of consent, identity verification, and contractual responsibility (Makarim, 2013). Under Indonesian civil law, the validity of contract remain fundamentally governed by article 1320 of the civil code, which

is requires the existence of consent, legal capacity, a specific object, and a lawful cause as essential elements of valid agreement. These legal requirements reflect the classical doctrine of contract law that emphasizes the existence of genuine intention and legal competence as prerequisites for the formation of binding legal obligations (Subekti, 2005).

However, the transition from conventional contracts to electronic contracts has created new legal challenges, particularly in verifying the identity and legal capacity of contracting parties in a digital environment (*Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions*, Article 5 paragraph (1)). In practice, electronic transactions frequently rely on automated systems that allow users to accept contractual terms by simply clicking and agreement button, commonly known as click-wrap agreement, without adequate verification of the user's legal competence or understanding of contractual terms (Winn and Wright, 2019). Previous legal research examining electronic contract in Indonesia has demonstrated that agreements entered into by minors through electronic systems possess a hight risk of legal invalidity due to the absence of legal capacity as a subjective requirement of contracts formation (Firmansyah, 2020). This condition highlights as a structural weakness in current electronic commerce systems that prioritize technological efficiency over the legal certainty and consumer protections (Radburch, 1950).

Furthermore, the absence of direct interaction between contracting parties in electronic transactions eliminates traditional mechanisms of verifications that were historically performed by legal professionals, particularly notaries, who function as public officials responsible for verifying identity and ensuring the authenticity of legal acts (Law of the Republic of Indonesia Number 2 of 2014 concerning the Office of Notary, Article 15 paragraph (1)). As electronic commerce continues to expand both domestic and international markets, the need for a reliable legal authentication mechanism becomes increasingly urgent to maintain trust and stability in digital (this stuffy therefore seeks to reconstruct the role of notaries within the digital economy by proposing a Notary-Based Digital Authentication Model (NDAM) that integrates legal verification procedures into electronic commerce systems. The proposes model aims to strengthen legal certainty, enhance consumer protection, and provide a normative framework for regulating digital transactions in accordance with fundamental principles of contract law.

Research Method and Theoretical Framework

This research employs a normative juridical method, which focuses on the analysis of legal norms contained in statutory regulations, judicial decisions, and legal doctrines as primary sources of legal reasoning (Soekanto and Mamudji, 2011) . Normative legal research is particularly appropriate for examine the validity of electronic contracts because the primary objective of this study is to evaluate the consistency between existing legal norms and the practical realities of digital transactions in contemporary society (Marzuki, 2017). The research adopts three principal approaches, namely the statutory approach, the conceptual approach, and the comparative approach. The statutory approach is used to analyze the legal framework governing electronic contracts, electronic signatures, and the authority of notaries under Indonesian Law, including the civil code, the law on Electronic Information and Transactions, and the Law on Notarial Office (Government Regulation of

the Republic of Indonesia Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, Article 3.).

The conceptual approach is utilized to examine fundamental legal doctrines such as legal certainty, legal protection, and trust in contractual relationships. Legal certainty is widely recognized as a core value in modern legal systems, ensuring that legal norms are predictable, consistent, and capable of providing guidance for human behaviour (Ali, 2010). According to the theory of legal certainty developed by Gustav Radbruch, the legitimacy of a legal system depends on its ability to maintain clarity and stability in legal norms while balancing the values of justice and utility (Radburch, 1932).

In addition, the theory of legal protection plays a crucial role in safeguarding the rights of vulnerable parties in electronic transactions, particularly minors and consumers who may lack sufficient legal awareness or bargaining power (Hadjon, 1987). Legal protection may be categorized into preventive protection, which aims to prevent disputes before they arise, and repressive protection, which seeks to resolve disputes through judicial mechanisms (Rahardjo, 2000).

The comparative approach is applied to analyze regulatory frameworks governing digital authentication and electronic transactions in selected jurisdictions, including Singapore, Malaysia, the United States, and the United Kingdom. Comparative legal analysis provides valuable insights into best practices and institutional models that may be adapted to strengthen the Indonesian legal system in the context of digital commerce (Zweigert and Kötz, 1998).

Result and Discussion

Legal Validity of Electronic Contracts Under Indonesian Law

The recognition of electronic contracts within Indonesian law represents a significant step toward harmonizing national legal systems with global technological developments. The enactment of Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended by Law No. 19 of 2016, formally acknowledges electronic information and electronic documents as legitimate legal evidence within judicial proceedings. This recognition reflects the state's commitment to adapting traditional legal frameworks to the realities of digital commerce and technological innovation.

Nevertheless, the formal recognition of electronic contracts does not eliminate the requirement that such contracts must comply with fundamental principles of contract law. In particular, the requirement of legal capacity remains an essential condition for the validity of any agreement, whether concluded through conventional or electronic means. Indonesian contract law continues to rely on the classical doctrine contained in Article 1320 of the Civil Code, which establishes four essential elements of a valid contract: consent, legal capacity, a specific object, and a lawful cause.

Legal capacity occupies a central role within this doctrinal structure because it determines whether an individual possesses the authority to create binding legal obligations. Under Indonesian law, individuals who have not reached the age of majority are considered legally incapable of entering into binding contracts without the consent of

their legal guardians. Consequently, contracts executed by minors may be declared voidable upon request by the minor or their legal representative, reflecting the legal system's commitment to protecting individuals who lack full legal competence.

In the context of electronic commerce, the verification of legal capacity presents a significant challenge because digital platforms often rely on self-declared information provided by users without independent validation. This reliance on unverified data increases the risk of fraudulent transactions and undermines the reliability of electronic contracts as legally binding instruments. The absence of reliable verification mechanisms also creates uncertainty for business operators who may unknowingly enter into contracts with individuals lacking legal capacity.

Furthermore, the widespread use of standardized contract terms in electronic commerce has created an imbalance of power between business operators and consumers, particularly when contractual terms are presented in complex legal language that may not be easily understood by users. Such practices raise concerns regarding the authenticity of consent in electronic contracts, as genuine consent requires both knowledge and understanding of the contractual obligations being accepted. Without adequate comprehension, the act of clicking an agreement button cannot be interpreted as a manifestation of true contractual intent.

Structural Weaknesses of Digital Contract Formation

One of the principal weaknesses of digital contract formation lies in the absence of a robust identity assurance mechanism that can reliably connect the person operating a device or account with the legal subject recognized by law. In many electronic commerce systems, identification is based only on usernames, passwords, telephone numbers, or email accounts, all of which may be borrowed, falsified, or misused without immediate detection (Maskun, 2013). As a result, the system may record apparent consent while remaining unable to prove that the real contracting party is the person legally attributed to the transaction (OECD, 2022)

A second weakness concerns the inability of most digital platforms to assess legal capacity at the moment of contract formation (Firmansyah, 2020). The issue is particularly acute in transactions involving minors, persons under guardianship, or persons acting on behalf of corporations without proper authorization, because the platform interface usually treats all users as formally equivalent without conducting legal qualification (Firmansyah, 2020). This creates a structural gap between the efficiency of digital contracting and the doctrinal demands of contract law, which still requires that a party be legally competent before obligations may arise validly in his, her, or its own name (Indonesian Civil Code Article 1320).

A third weakness arises from the reduction of consent into a mechanical act of interface interaction (Winn and Wright, 2019). Click-wrap agreements may be commercially efficient, but efficiency alone does not guarantee that consent is informed, deliberate, or legally meaningful (Subekti, 2005). Where the system is designed to prioritize speed, scalability, and automated user onboarding, there is a serious risk that the legal act of

agreement becomes detached from its substantive juridical meaning (UNCTAD, 2023). These weaknesses show that the current structure of many digital contracting systems remains technologically functional but legally incomplete. If legal certainty is to be preserved, the law requires an intermediary verification model capable of restoring accountability, traceability, and legally reliable assent without destroying the practical advantages of digital commerce.

The Role of Notaries In Digital Transactions

Notaries hold a distinctive institutional position within civil law systems because they function not merely as witnesses to private acts, but as public officials entrusted with verifying identity, legal capacity, and the formal authenticity of legal instruments (Law of the Republic of Indonesia Number 2 of 2014 concerning the Office of Notary, Article 15 paragraph (1)). In Indonesian law, this authority is expressly recognized by the Law on Notarial Office, which gives notaries competence to perform authenticating functions that carry enhanced evidentiary value. Because the central problems of electronic contracts concern identity, capacity, authenticity, and proof, the notarial office is normatively relevant to the digital contracting environment.

In this digital era, the adaptation of notarial functions should be understood as a functional extension rather than an institutional replacement (Makarim, 2013). The idea of cyber notary does not remove the legal character of the notary as a public official; instead, it extends the verification and authentication function into an electronic environment where parties may no longer meet physically but still require trustworthy legal validation (Makarim, 2013). This makes the notary particularly suitable to operate as a legally accountable trust intermediary within digital transaction systems (Indonesian Notary Association, 2022).

The integration of notarial procedures into electronic commerce may improve legal certainty in at least four ways. First, the notary can verify the legal identity of the parties through recognized documentation and secure digital authentication tools Second, the notary can assess legal capacity, including minority status, guardianship, or representative authority in corporate transactions. Third, the notary can authenticate the integrity and attribution of the electronic contract. Fourth, the notary can validate the legal reliability of the electronic signature used in the transaction.

The preventive value of notarial involvement is also significant. By verifying the core elements of contract formation at the outset, the notary may reduce disputes concerning impersonation, unauthorized agreement, invalid capacity, and evidentiary authenticity. In this sense, the role of the notary in digital transactions is not merely ceremonial, but structurally important for restoring trust to electronic commerce.

Comparative Analysis of Digital Authentication Systems

Comparative legal analysis demonstrates that jurisdictions with mature digital economies do not rely solely on formal recognition of electronic signatures; they also develop institutional systems for identity assurance, authentication governance, and digital

trust (Zweigert and Kötz, 1998). The experiences of Singapore, Malaysia, the United States, and the United Kingdom show that the legal sustainability of electronic commerce depends on the interaction between statutory recognition, technical infrastructure, and accountable intermediary mechanisms.

1. Singapore

Singapore has established a comprehensive legal framework for electronic transactions through the Electronic Transactions Act, which recognizes electronic signatures and digital records as legally valid instruments. The government has also developed the SingPass digital identity system, enabling citizens to authenticate their identity securely when accessing online services and conducting electronic transactions. SingPass functions as a centralized digital identity infrastructure that integrates government databases with private sector services, thereby ensuring consistent identity verification standards across multiple platforms.

2. Malaysia

Malaysia regulates digital transactions through the Digital Signature Act and the Electronic Commerce Act, both of which emphasize the importance of secure authentication mechanisms in protecting consumers and maintaining trust in electronic commerce. The introduction of the MyDigital ID system further demonstrates the government's commitment to strengthening digital identity infrastructure. MyDigital ID utilizes advanced encryption technology to ensure data integrity and prevent unauthorized access to personal information.

3. United states

The United States recognizes the legal validity of electronic contracts through the Electronic Signatures in Global and National Commerce Act (E-SIGN Act), which establishes that electronic signatures possess the same legal effect as handwritten signatures. In addition to statutory regulation, the National Institute of Standards and Technology (NIST) has developed technical guidelines for digital identity verification, providing a standardized framework for authentication processes within electronic systems. These guidelines emphasize risk-based verification procedures designed to balance security requirements with user convenience (NIST)

4. United kingdom

The United Kingdom regulates electronic communications through the Electronic Communications Act, which grants legal recognition to digital signatures and electronic documents. The government-operated GOV.UK Verify system enables citizens to confirm their identity online through accredited identity providers. This decentralized verification model allows private entities to participate in the authentication process while maintaining government oversight and regulatory compliance (European Union Regulation (EU) No. 910/2014)

The comparative analysis demonstrates that advanced digital economies rely on structured identity verification systems supported by clear legal authority and institutional accountability. These systems illustrate the importance of integrating technological infrastructure with legal governance to ensure the reliability of electronic transactions.

Notary Based Digital Authentication Model (NDAM)

The Notary-Based Digital Authentication Model (NDAM) is proposed as a normative reconstruction designed to integrate public legal verification into the architecture of electronic commerce (Indonesian Notary Association, 2022). The model is based on the premise that digital contracting should not depend solely on technical interaction or platform-generated acceptance, but must be supported by a legally accountable process capable of confirming identity, capacity, authenticity, and valid asset. In that sense, NDAM does not negate the convenience of digital transactions; rather, it supplements technological efficiency with institutional legality.

The first component of NDAM is digital identity verification (OECD, 2022). This component aims to ensure that the person entering the electronic system is the same person legally recognized in the transaction, thereby reducing the risks of impersonation, account misuse, and fraudulent attribution (OECD, 2022). The second component is legal capacity assessment, which is particularly important for detecting whether the user is a minor, a person under guardianship, or a representative whose authority depends upon organizational authorization (Firmansyah, 2020). The third component is contract authentication.[33] This refers to the legal confirmation that the electronic document is complete, attributable to the identified parties, and protected against unauthorized alteration after agreement.[33] The fourth component is electronic signature validation, which ensures that the digital form of assent used by the parties satisfies legal and technical standards necessary for evidentiary reliability and enforceability. Normatively, NDAM is intended to function as a bridge between classical contract doctrine and contemporary digital practice.

By incorporating the notary as a trusted public intermediary, the model is expected to reduce fraud, strengthen consumer confidence, and improve the enforceability of electronic agreements in both domestic and cross-border transactions. It therefore serves as a reconstruction framework that aligns technological development with the legal values of certainty, protection, responsibility, and trust.

Conclusion

The expansion of digital commerce has transformed the mechanics of contracting, but it has not displaced the continuing relevance of the classical legal requirements of consent, legal capacity, certainty of object, and lawful cause. What has changed is the environment in which these requirements must now be verified, interpreted, and protected. Indonesian law has already recognized electronic information, electronic documents, and electronic signatures as legally effective, yet this recognition remains incomplete where the legal system lacks a reliable mechanism for verifying who the parties are and whether they are legally competent to bind themselves.[5] The analysis in this study shows that the central weakness of many electronic contracting systems lies not in the absence of law, but in the absence of a trustworthy institutional verification structure capable of connecting technological transactions with legal accountability.

The proposed Notary-Based Digital Authentication Model responds to this weakness by repositioning the notary as a digital trust authority who can verify identity, assess capacity, authenticate contracts, and validate electronic signatures within a legally accountable framework. Accordingly, NDAM should be understood as a normative reconstruction rather than a purely technical proposal. By combining notarial verification with digital authentication, the model offers a realistic pathway for improving legal certainty, preventive protection, and public trust in Indonesia's electronic commerce system. Its adoption would not only strengthen contract validity in domestic transactions, but also place Indonesian digital commerce within a more credible comparative framework aligned with international developments in digital trust governance.

References

Ali, A. (2010). Menguak teori hukum (Legal theory). Kencana.

American Bar Association. (2020). Electronic transactions and digital law practice. American Bar Association.

Asian Development Bank. (2022). Digital governance framework. Asian Development Bank.

Danul Firmansyah, A. (2020). Kepastian hukum perjanjian elektronik dalam perdagangan melalui sistem elektronik yang ditandatangani oleh anak di bawah umur (Master's thesis, Universitas Jayabaya).

European Union. (2014). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

Hadjon, P. M. (1987). Perlindungan hukum bagi rakyat Indonesia. Bina Ilmu.

Horton, D. (2017). Clickwrap agreements and consumer protection. University of Pennsylvania Law Review.

Ikatan Notaris Indonesia. (2022). Cyber notary concept paper. Ikatan Notaris Indonesia.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2026). Regulasi sistem elektronik. Retrieved April 23, 2026, from Kementerian Komunikasi dan Informatika Republik Indonesia

Makarim, E. (2013). Notaris dan transaksi elektronik: Kajian hukum tentang cybernotary atau electronic notary. Rajawali Pers.

Malaysia. (1997). Digital Signature Act 1997.

Nurhayani, N. Y. (2015). Hukum perdata. Pustaka Setia.

Organisation for Economic Co-operation and Development (OECD). (2022). Digital identity framework 2022. OECD.

Rahardjo, S. (2006). Ilmu hukum. Citra Aditya Bakti.

Ramli, A. M. (2004). Cyber law dan HAKI dalam sistem hukum Indonesia. Refika Aditama.

Reed, C. (2018). Making laws for cyberspace. Oxford Journal of Legal Studies.

Shidarta. (2006). Moralitas profesi hukum: Suatu tawaran kerangka berpikir. Refika Aditama.

Singapore. (n.d.). Electronic Transactions Act (Cap 88).

Soekanto, S., & Mamudji, S. (2011). Penelitian hukum normatif: Suatu tinjauan singkat. RajaGrafindo Persada.

Subekti. (2005). Hukum perjanjian. Intermasa.

United Kingdom. (2000). Electronic Communications Act 2000.

United Nations Commission on International Trade Law (UNCITRAL). (1996). Model law on electronic commerce 1996.

United Nations Commission on International Trade Law (UNCITRAL). (2001). Model law on electronic signatures 2001.

United Nations Conference on Trade and Development (UNCTAD). (2023). Digital economy report 2023. UNCTAD.

United States. (2000). Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001.

Winn, J. K., & Wright, B. (2019). The law of electronic commerce. Aspen Publishers.

World Bank. (2023). Digital development overview 2023. World Bank.

World Economic Forum. (2023). Digital trust framework 2023. World Econo