Lex Recta: Journal of Law and Normative Justice
Vol 1 No 2 June 2026, Hal 13-24
ISSN: XXXX-XXXX (Print) ISSN: XXXX-XXXX (Electronic)
Open Access: https://sovereignresearch.org/lex-recta

Legal Recognition of Digital Identity in Cross-Border Electronic Transactions: Reconstructing Normative Frameworks for Legal Certainty

Andi Hartawati[1*], Toman Sony Tambunan[2], Elva Mahmudi[3]
[1] Universitas Andi Sudirman, Indonesia
[2] Universitas HKBP Nommensen Medan, Indonesia
[3] STAIN Mandailing Natal, Indonesia
email: ahartawati@gmail.com[1]

Article Info :
Received:
20-05-2026
Revised:
27-05-2026
Accepted:
08-06-2026

Abstract

This study examines the legal recognition of digital identity in cross-border electronic transactions and evaluates its significance for the establishment of legal certainty within contemporary digital commerce. The rapid expansion of transnational electronic trade has exposed structural weaknesses in existing legal frameworks, particularly regarding the attribution, authentication, and recognition of digital identities across different jurisdictions. Employing a normative, doctrinal, and comparative legal approach, the research analyzes international legal instruments, Indonesian legislation, regulatory frameworks on electronic signatures and trust services, and comparative models of digital identity governance. The analysis demonstrates that current regulations primarily emphasize technological authentication and transactional validity while providing insufficient mechanisms for mutual legal recognition of digital identities across borders. Jurisdictional fragmentation, regulatory divergence, and inconsistencies in evidentiary recognition generate uncertainty concerning contractual enforceability, accountability, consumer protection, and cross-border regulatory enforcement. The study proposes a reconstructed normative framework founded upon mutual recognition, regulatory equivalence, legal attribution, data protection integration, and procedural enforceability. This framework reconceptualizes digital identity as a transnational legal institution capable of supporting interoperability, accountability, and legal certainty within the evolving architecture of global electronic commerce.

Keywords: *Digital Identity, Cross-Border Transactions, Legal Recognition, Legal Certainty, Regulatory Harmonization.*

INTRODUCTION

The accelerated expansion of cross-border electronic transactions has fundamentally transformed the architecture of global commerce, shifting economic interactions from territorially bounded exchanges toward digitally mediated ecosystems in which parties may transact without ever sharing a common jurisdiction, regulatory environment, or institutional infrastructure. Within this transformation, digital identity has emerged as a foundational legal and technological instrument because the validity of electronic consent, authentication of contracting parties, attribution of legal acts, and enforceability of obligations increasingly depend upon reliable mechanisms capable of verifying identity across heterogeneous legal systems. Contemporary developments in digital trade governance reveal a growing convergence between digital identity frameworks, electronic signature infrastructures, and transnational data governance regimes, reflecting a broader recognition that legal certainty in cross-border electronic transactions cannot be achieved solely through contractual autonomy or technological innovation. Scholarly discussions concerning the legal validity of digital signatures, the evolution of electronic agreements, and the institutional design of unified digital identity systems consistently emphasize that identity verification constitutes the normative gateway through which trust, accountability, and legal recognition are constructed within digital markets (Susilowati et al., 2025; Abhipraya et al., 2025; Utomo et al., 2025).

Existing scholarship has generated important insights into the relationship between digital identity, electronic contracting, and transnational commerce, although the dominant analytical orientation remains fragmented across distinct doctrinal and regulatory domains. Studies examining the legal validity of digital signatures have demonstrated the necessity of authentication mechanisms for establishing evidentiary reliability in electronic transactions, while research on digital identity convergence has proposed the institutional integration of technological and legal infrastructures as a means of strengthening virtual economic ecosystems (Susilowati et al., 2025; Utomo et al., 2025). Parallel investigations into cross-border e-commerce have highlighted the vulnerability of consumers operating within transnational digital marketplaces, particularly where jurisdictional asymmetries and divergent regulatory standards complicate dispute resolution and legal protection (Heng & Lie, 2025; Rahmatullah & Subair, 2024; Luviana & Pratiwi, 2026). Complementary analyses of smart contracts have further demonstrated that anonymity and pseudonymity embedded within digital environments challenge conventional doctrines of legal attribution, thereby elevating the significance of digital identity as a prerequisite for determining rights, obligations, and liability (Situmorang & Salam, 2025). Collectively, these studies suggest that digital identity performs functions extending far beyond technical authentication, operating instead as a normative mechanism through which legal personality is translated into digitally recognizable forms.

Despite these contributions, the existing literature exhibits several conceptual limitations that impede the development of a coherent framework for legal recognition of digital identity in cross-border contexts. A significant portion of the scholarship remains focused on domestic regulatory arrangements and national legal validity standards, resulting in analyses that inadequately address the complexities arising when electronic transactions traverse multiple jurisdictions with differing approaches to identity verification, evidentiary recognition, and regulatory compliance (Susilowati et al., 2025; Agusnur, 2025). Research addressing consumer protection and cross-border digital commerce frequently identifies legal risks associated with transnational transactions, yet often treats identity verification as a subsidiary technical issue rather than as an autonomous legal institution capable of determining the enforceability of transnational legal relationships (Heng & Lie, 2025; Rahmatullah & Subair, 2024; Luviana & Pratiwi, 2026). Equally problematic is the tendency of studies on digital identity governance to emphasize institutional design and technological integration without sufficiently interrogating the normative conditions under which digital identities generated in one jurisdiction may obtain legal recognition in another (Utomo et al., 2025). The resulting body of literature reveals a persistent disconnect between technological interoperability and legal interoperability, leaving unresolved the question of how legal certainty can be maintained when digital identities operate across divergent normative systems.

The unresolved nature of this issue possesses both scientific and practical significance because the absence of universally recognized legal standards governing cross-border digital identity directly affects contractual validity, evidentiary reliability, consumer protection, cybercrime prevention, and transnational regulatory enforcement. Increasing reliance on digital platforms, decentralized technologies, and automated contractual mechanisms has intensified situations in which the legal status of a digital identity remains uncertain despite the technical authenticity of the underlying transaction. Such uncertainty generates systemic risks by creating ambiguities concerning attribution of conduct, determination of jurisdiction, allocation of liability, and recognition of electronic evidence, particularly in transactions involving parties located across multiple sovereign legal orders. Contemporary challenges associated with cross-border cyber activities further illustrate how fragmented legal recognition frameworks can undermine enforcement effectiveness and weaken accountability structures within digital ecosystems (Islami, 2025). The persistence of these challenges indicates that technological advancement alone cannot resolve the normative tensions inherent in transnational digital interactions, particularly when legal systems continue to operate according to territorially bounded assumptions that are increasingly incompatible with digitally networked economic relations.

The present study is situated within an emerging body of scholarship seeking to move beyond technology-centric and jurisdiction-specific analyses toward a more integrated examination of digital identity as a transnational legal institution. Rather than focusing exclusively on the validity of electronic signatures, consumer protection mechanisms, or digital governance architecture, this research conceptualizes legal recognition of digital identity as a foundational normative problem that lies at the intersection of private law, public regulation, digital governance, and cross-border legal harmonization. Such a perspective responds directly to the fragmentation observable within existing literature by examining how legal systems construct, recognize, and legitimize digital identity across jurisdictional boundaries, while simultaneously assessing the extent to which prevailing legal frameworks are capable of supporting legal certainty in increasingly interconnected digital markets. The study therefore addresses a critical gap concerning the normative relationship between identity recognition, legal attribution, and transnational enforceability in electronic transactions.

This research aims to reconstruct the normative framework governing the legal recognition of digital identity in cross-border electronic transactions in order to strengthen legal certainty within transnational digital commerce. The study develops a theoretical model that repositions digital identity from a merely technical authentication tool into a legally recognized transnational institution capable of facilitating legal attribution, contractual validity, and regulatory accountability across jurisdictions. Methodologically, the research advances an integrative normative approach that combines doctrinal analysis, comparative legal reasoning, and transnational regulatory evaluation to formulate a coherent framework for cross-border digital identity recognition. The anticipated contribution lies in providing a conceptual foundation for future legal harmonization initiatives while offering a more systematic analytical framework for understanding the relationship between digital identity, legal certainty, and the evolving architecture of global electronic transactions.

RESEARCH METHODS

This study constitutes a non-empirical legal research employing a normative and doctrinal approach, complemented by a comparative legal perspective, to examine the legal recognition of digital identity in cross-border electronic transactions. The research is grounded primarily in secondary legal materials, including international legal instruments governing electronic commerce and digital trade, national legislation on electronic transactions and digital identity systems, regulatory frameworks concerning electronic signatures and trust services, as well as scholarly literature addressing digital governance, transnational commercial law, legal certainty, and cross-border regulatory harmonization. Comparative examination is undertaken to identify convergences and divergences among existing legal frameworks concerning the recognition, authentication, and legal effects of digital identities across different jurisdictions, thereby enabling a systematic assessment of the normative challenges associated with transnational digital interactions.

The analytical framework is based on doctrinal legal analysis integrated with conceptual and comparative interpretation. Legal norms are examined through statutory, systematic, and teleological interpretation to evaluate their coherence, consistency, and capacity to provide legal certainty in cross-border electronic transactions. The study further employs a normative reconstruction method to identify regulatory gaps, jurisdictional inconsistencies, and conceptual deficiencies within existing legal frameworks governing digital identity recognition. Through comparative synthesis and legal reasoning, the analysis develops a reconstructed normative framework aimed at strengthening transnational legal recognition of digital identities, enhancing legal attribution mechanisms, and promoting greater certainty, interoperability, and accountability within the evolving architecture of global digital commerce.

RESULTS AND DISCUSSION

Normative Foundations of Digital Identity Recognition in Cross-Border Electronic Transactions

The legal recognition of digital identity has evolved from a purely technological mechanism of authentication into a juridical construct that determines whether a person, entity, or legally attributable actor can exercise rights and assume obligations within electronically mediated legal relations. Article 6 of the UNCITRAL Model Law on Electronic Commerce establishes functional equivalence between electronic and paper-based information, while Article 7 recognizes electronic signatures when reliability requirements are satisfied, thereby introducing a normative basis for legal attribution in digital environments. Article 25 of the eIDAS Regulation further strengthens this approach by providing legal effect to qualified electronic signatures equivalent to handwritten signatures under European Union law. Doctrinal analysis demonstrates that these instruments implicitly depend upon legally recognizable digital identities because attribution of electronic acts cannot occur in the absence of a verifiable juridical subject capable of being connected to the transaction in question (Sullivan, 2018). Scholarly arguments concerning the transition from traditional legal personality toward digitally mediated identity frameworks indicate that digital identity now functions as an independent legal institution rather than a mere evidentiary tool supporting contractual validity (Sullivan, 2018; Sharma, 2025).

A systematic interpretation of Indonesian law reveals that legal recognition of digital identity remains dispersed across multiple regulatory instruments rather than consolidated within a single normative framework. Article 1 point 12 and Article 11 of Law No. 11 of 2008 on Electronic Information and Transactions as amended by Law No. 1 of 2024 regulate electronic signatures, whereas Article 1 point 21 defines electronic certificates as instruments connecting identity data with verification systems. Government regulation through Government Regulation No. 71 of 2019 introduces obligations concerning electronic authentication and trust services, yet does not comprehensively define the transnational legal consequences of digital identity recognition. Comparative reading of these provisions suggests that Indonesian law primarily regulates technological validity rather than legal interoperability between domestic and foreign identity systems. Such fragmentation supports the argument advanced by Utomo et al. (2025) that digital identity governance remains institutionally incomplete despite increasing dependence upon digital trade ecosystems.

The relationship between digital identity and legal certainty must be examined through the lens of legal attribution because enforceability of electronic transactions presupposes a legally identifiable actor. Article 8 of the UNCITRAL Model Law on Electronic Commerce and Article 12 of the UNCITRAL Model Law on Electronic Signatures recognize reliability and attribution as essential conditions for legal effectiveness. Functional equivalence principles become normatively deficient when identity recognition mechanisms differ substantially across jurisdictions, particularly where one jurisdiction recognizes identity credentials that another jurisdiction refuses to acknowledge. Comparative legal scholarship demonstrates that electronic authentication systems often satisfy technological reliability standards while failing to achieve reciprocal legal recognition among sovereign legal orders (Andraško & Mesarčík, 2021). This divergence creates a structural tension between technological interoperability and juridical legitimacy that remains insufficiently addressed within contemporary electronic commerce regulation.

The significance of this normative tension becomes more apparent when examined through developments in electronic contracting. Contract formation under digital conditions no longer depends primarily upon physical presence or documentary formalities but increasingly relies upon electronic authentication processes capable of linking contractual declarations to identifiable legal subjects. Studies concerning the evolution of electronic contracts indicate that consent, intention, and attribution are increasingly mediated through identity verification infrastructures rather than conventional evidentiary mechanisms (Abhipraya et al., 2025; Hebat & Hidayat, 2026). Teleological interpretation of electronic transaction legislation demonstrates that legal certainty requires not only technological authentication but also predictable recognition of digital identity across borders. Juridical certainty consequently depends upon the existence of normative standards governing recognition rather than merely technical standards governing verification.

A comparative review of international frameworks reveals divergent regulatory philosophies regarding digital identity governance. The European Union adopts a harmonized recognition model through eIDAS, while several Asian jurisdictions continue to rely upon sectoral or fragmented identity regulations. International trade law instruments increasingly acknowledge the importance of trusted digital identities without establishing a universally binding legal recognition regime.

Research concerning electronic transferable records and cross-border trade digitalization demonstrates that legal modernization efforts often prioritize transactional efficiency while postponing questions concerning transnational identity legitimacy (ALsheyab, 2025). Such regulatory asymmetry creates uncertainty regarding whether an authenticated identity in one jurisdiction retains equivalent legal status in another jurisdiction. The doctrinal deficiencies within existing legal frameworks may be mapped through the following comparative normative matrix:

Table 1. Comparative Normative Frameworks Governing Digital Identity Recognition in Cross-Border Electronic Transactions

Legal Instrument	Identity Function	Recognition Scope	Normative Limitation
UNCITRAL Model Law on Electronic Commerce 1996	Attribution and authentication	International reference model	Non-binding implementation

Legal Instrument	Identity Function	Recognition Scope	Normative Limitation
eIDAS Regulation 910/2014	Qualified electronic identification	European Union	Limited extraterritorial effect
Indonesian ITE Law	Electronic signature validity	National jurisdiction	No comprehensive cross-border recognition
PP No. 71/2019	Trust services regulation	National electronic systems	Fragmented interoperability framework

The table demonstrates that legal systems generally recognize authentication mechanisms while leaving unresolved the broader question of mutual legal recognition. Normative comparison indicates that existing instruments regulate the validity of digital acts more comprehensively than the legal status of digital identities themselves. The distinction between transaction validity and identity recognition becomes particularly significant in transnational legal relations involving multiple regulatory authorities. Doctrinal coherence remains difficult to achieve where legal systems employ different criteria for recognizing digitally authenticated persons and entities.

Consumer protection literature reinforces this concern by demonstrating that legal uncertainty frequently originates from difficulties in identifying accountable parties rather than from technological failures. Cross-border electronic commerce disputes often involve conflicting assumptions concerning jurisdiction, contractual enforceability, and evidentiary attribution because digital identities are recognized differently across legal systems (Rahmatullah & Subair, 2024; Heng & Lie, 2025). Article 18 of the Indonesian ITE Law recognizes electronic contracts, yet practical enforceability depends upon the ability to identify legally responsible actors within foreign jurisdictions. Studies on consumer protection in digital commerce consistently reveal that legal remedies become significantly weaker when identity verification systems lack transnational recognition mechanisms (Agusnur, 2025; Fitriani et al., 2025). Legal certainty therefore requires a normative architecture capable of linking identity recognition with accountability structures extending beyond territorial boundaries.

The emergence of decentralized technologies introduces additional complexity into the legal recognition debate. Distributed ledger systems enable authentication without centralized intermediaries, creating tensions between technological autonomy and legal accountability. Regulatory scholarship concerning blockchain-based registries and digital legal certainty argues that decentralized identity systems may enhance transactional integrity while simultaneously complicating attribution and jurisdictional determination (Espinal De Aza, 2023; Zetzsche et al., 2021). Doctrinal analysis suggests that traditional legal concepts concerning personhood and identification require reinterpretation when identity credentials are generated and validated through decentralized infrastructures. Existing legal frameworks remain insufficiently equipped to address this transformation because they were largely designed around centralized verification architectures.

Questions of data protection further complicate the legal status of digital identity in cross-border transactions. Digital identity systems inevitably involve processing personal data across multiple jurisdictions, thereby implicating competing regulatory standards concerning privacy, disclosure, and lawful processing. Comparative studies concerning electronic identification and cross-border data governance demonstrate that legal recognition mechanisms cannot be separated from broader obligations concerning data protection and informational self-determination (Andraško & Mesarčík, 2021; Azam et al., 2026). Indonesian regulatory developments concerning personal data protection reveal ongoing efforts to reconcile digital economic growth with legal safeguards protecting individual rights (Kaplale & Maulana, 2026). Normative coherence consequently requires integration between identity recognition rules and data governance frameworks rather than treating them as independent regulatory domains.

The doctrinal trajectory emerging from these legal instruments, judicial principles, and scholarly analyses suggests that digital identity should be conceptualized as a transnational legal status rather than a domestic technological credential. Legal certainty in cross-border electronic transactions depends upon recognition mechanisms capable of ensuring continuity of identity across different legal systems without undermining sovereignty or regulatory autonomy. Interpretative analysis of international electronic commerce norms demonstrates that attribution, authentication, enforceability, and accountability are functionally interconnected dimensions of a single legal problem concerning identity recognition (Susilowati et al., 2025; Savita et al., 2025). Contemporary legal transformation increasingly requires movement beyond fragmented regulatory approaches toward frameworks capable of establishing mutual recognition and normative interoperability (Taufani & Negara, 2026; Toyi & Hamidun, 2025). The doctrinal foundation developed in this section establishes the analytical basis for examining how jurisdictional conflicts and cross-border legal fragmentation affect the practical operation of digital identity recognition in transnational electronic transactions.

Jurisdictional Fragmentation and the Legal Challenges of Cross-Border Digital Identity Recognition

Jurisdiction constitutes one of the most contested dimensions of digital identity recognition because the legal validity of an electronic identity frequently depends upon regulatory assumptions that remain territorially bounded despite the inherently transnational nature of digital transactions. Traditional private international law was developed upon the premise that legal relationships could be connected to identifiable territorial factors such as domicile, place of contracting, place of performance, or location of assets. Cross-border electronic transactions increasingly disrupt these connecting factors because contractual communications, identity verification processes, data storage infrastructures, and payment systems may simultaneously operate across multiple jurisdictions. Article 18 paragraph (4) of the Indonesian ITE Law permits parties to determine governing law in electronic contracts, yet the provision does not directly address whether a digital identity legally recognized in one jurisdiction must be accepted as valid in another jurisdiction. Comparative legal scholarship indicates that jurisdictional uncertainty often emerges not from disagreement concerning contract validity but from disagreement concerning the legal identity of the contracting parties themselves (Ming-zhe et al., 2025).

The legal consequences of fragmented identity recognition become particularly apparent when examining attribution of electronic conduct across borders. Article 13 of the UNCITRAL Model Law on Electronic Commerce establishes principles regarding attribution of data messages to an originator, while Article 6 of the UNCITRAL Model Law on Electronic Signatures links attribution to reliable authentication mechanisms. Doctrinal interpretation reveals that these provisions presuppose a degree of confidence concerning the legal status of the identified person, yet they do not establish binding rules requiring mutual recognition of digital identities among sovereign jurisdictions. A legally valid electronic identity credential issued in one country may therefore encounter evidentiary or regulatory obstacles when presented before administrative authorities or courts in another country. This gap demonstrates that attribution rules alone cannot guarantee legal certainty where identity recognition remains fragmented at the jurisdictional level.

A comparative examination of the European Union framework highlights the importance of regulatory harmonization in reducing identity-related jurisdictional disputes. Regulation (EU) No. 910/2014 establishes mutual recognition obligations concerning notified electronic identification schemes among Member States, thereby reducing uncertainty regarding the legal effect of digital identities within the European internal market. Article 6 of the eIDAS Regulation creates a recognition mechanism extending beyond technical interoperability by imposing normative obligations upon participating jurisdictions. Legal analysis demonstrates that this model addresses not only authentication reliability but also legal continuity of identity across borders. The European approach illustrates how legal certainty can be strengthened when recognition is treated as a juridical obligation rather than a discretionary administrative decision (Andraško & Mesarčík, 2021).

The Indonesian regulatory framework presents a different configuration because legal recognition remains concentrated upon validity of electronic signatures and electronic documents rather than reciprocal recognition of foreign digital identities. Article 59 of Government Regulation No. 71 of 2019 recognizes electronic certification services, while Article 60 regulates reliability requirements for trust service providers. Systematic interpretation suggests that these provisions establish domestic standards for authentication without creating a comprehensive mechanism governing recognition of foreign-issued identity credentials.

Juridical uncertainty consequently arises whenever cross-border transactions involve authentication systems developed under foreign legal frameworks. Scholarly assessments of Indonesian digital governance consistently identify interoperability deficiencies as a central obstacle to effective participation in transnational digital trade environments (Utomo et al., 2025). The practical dimensions of jurisdictional fragmentation may be illustrated through the following normative comparison:

Table 2. Comparative Analysis of Electronic Identity Recognition Regimes between the European Union and Indonesia

Regulatory Dimension	European Union (eIDAS)	Indonesia (ITE Law & PP 71/2019)	Legal Consequence
Electronic Identity Recognition	Mutual recognition obligation	No comprehensive reciprocal recognition regime	Divergent legal status
Authentication Standards	Harmonized regional framework	Domestic trust-service regulation	Limited interoperability
Cross-Border Legal Effect	Explicitly regulated	Implicit and fragmented	Jurisdictional uncertainty
Evidentiary Recognition	Integrated framework	Case-dependent assessment	Inconsistent enforcement

The table demonstrates that regulatory divergence extends beyond technical architecture and directly affects legal certainty. Mutual recognition mechanisms create predictability concerning legal status, whereas fragmented frameworks require case-by-case evaluation of foreign credentials. Judicial and administrative authorities consequently possess broader discretion in determining evidentiary value and legal validity. Such discretion may undermine transactional certainty when parties cannot reliably predict whether their identities will receive equivalent legal recognition abroad.

The emergence of smart contracts intensifies these jurisdictional difficulties because automated transactions often operate without direct human intervention after deployment. Legal scholarship concerning digital assets and smart contracts emphasizes that anonymity and pseudonymity complicate attribution, responsibility, and enforcement when disputes arise (Situmorang & Salam, 2025). Doctrinal analysis indicates that smart contract execution may satisfy technological requirements for performance while simultaneously creating uncertainty regarding identification of legally accountable actors. Traditional conflict-of-laws principles encounter significant challenges when contractual obligations are executed through decentralized infrastructures distributed across multiple jurisdictions. Recognition of digital identity consequently becomes a prerequisite for determining whether legal obligations can be attributed to identifiable persons rather than merely to technological systems.

Cross-border consumer transactions provide another context in which jurisdictional fragmentation generates substantial legal consequences. Consumer protection norms generally rely upon the ability to identify traders, determine applicable law, and establish mechanisms for dispute resolution. Studies concerning cross-border electronic commerce demonstrate that difficulties in identifying foreign counterparties frequently prevent consumers from exercising legal remedies despite the existence of substantive rights under applicable legislation (Heng & Lie, 2025; Luviana & Pratiwi, 2026). Article 28G paragraph (1) of the Constitution of the Republic of Indonesia guarantees protection of personal security and legal certainty, values that become difficult to realize where digital identities cannot be reliably verified across borders. Effective consumer protection therefore depends not only upon substantive regulatory standards but also upon recognition systems capable of establishing legally attributable identities.

Jurisdictional fragmentation also affects enforcement of cybercrime legislation and digital investigations. Cross-border cyber incidents frequently involve actors operating through digital identities recognized differently across legal systems, creating evidentiary and procedural challenges during investigation and prosecution. Comparative legal studies concerning cybercrime jurisdiction and digital evidence admissibility demonstrate that inconsistent identity recognition standards often impede cross-border cooperation between enforcement authorities (Eswaramoorthi, 2026; Islami, 2025). Article 43 of the Indonesian ITE Law provides investigative authority concerning electronic offenses, yet practical implementation remains dependent upon access to reliable identification mechanisms.

Enforcement effectiveness consequently becomes linked to the existence of interoperable legal frameworks capable of supporting attribution across jurisdictions.

Data governance frameworks introduce additional jurisdictional tensions because identity verification frequently requires transnational movement of personal information. Regulatory approaches concerning cross-border data flows differ substantially regarding consent requirements, lawful processing standards, localization obligations, and supervisory oversight. Legal scholarship examining digital identity and cross-border data disclosure demonstrates that recognition mechanisms may conflict with privacy protections when identity verification requires extensive transfer of personal data across jurisdictions (Sullivan, 2014). Comparative analysis of international trade governance similarly indicates that legal regimes increasingly struggle to balance economic integration objectives with data sovereignty concerns (Azam et al., 2026). Jurisdictional fragmentation therefore reflects not merely procedural divergence but also competing conceptions concerning privacy, sovereignty, and regulatory authority.

Contemporary developments in digital commerce reveal that jurisdictional uncertainty increasingly threatens the predictability of transnational economic relations. Electronic transferable records, decentralized payment infrastructures, and digitally authenticated commercial transactions rely upon assumptions concerning recognition that remain only partially reflected within existing legal frameworks. Research addressing digital trade modernization demonstrates that transactional efficiency cannot be sustained indefinitely where identity recognition continues to depend upon fragmented national standards (ALsheyab, 2025; Zetzsche et al., 2021). Comparative interpretation of international legal instruments suggests that legal certainty requires recognition mechanisms extending beyond authentication and encompassing legal status, evidentiary value, and enforceability. Jurisdictional fragmentation consequently emerges as a structural challenge requiring normative reconstruction rather than isolated regulatory adjustments.

Reconstructing a Transnational Normative Framework for Digital Identity Recognition and Legal Certainty

The reconstruction of a transnational normative framework for digital identity recognition must begin with a conceptual reassessment of digital identity as a juridical status rather than a merely technological credential. Existing regulatory models predominantly focus on authentication reliability, cybersecurity compliance, and evidentiary admissibility, while insufficient attention is directed toward the legal continuity of identity across jurisdictions. A doctrinal reading of Article 7 of the UNCITRAL Model Law on Electronic Commerce, Article 6 of the UNCITRAL Model Law on Electronic Signatures, and Article 25 of the eIDAS Regulation reveals that legal systems already acknowledge the importance of trustworthy electronic identification mechanisms, although recognition remains confined within fragmented institutional boundaries. Theoretical developments concerning digital identity indicate that identity functions as the legal foundation upon which rights, obligations, and accountability structures are constructed in digital environments (Sullivan, 2018). Normative reconstruction consequently requires a shift from transaction-centered regulation toward identity-centered regulation capable of ensuring continuity of legal status across national legal systems.

A teleological interpretation of contemporary electronic commerce legislation demonstrates that legal certainty cannot be achieved solely through harmonization of electronic signatures and electronic documents. Article 1320 of the Indonesian Civil Code establishes consent and legal capacity as essential requirements of contractual validity, while Article 18 of the ITE Law extends contractual recognition to electronic environments. Legal capacity and contractual consent remain inseparable from reliable identification of the contracting party, creating a direct relationship between digital identity recognition and enforceability of legal obligations. Scholarly analyses concerning the evolution of electronic contracts consistently demonstrate that technological modernization of contract law has outpaced the development of transnational identity governance mechanisms (Abhipraya et al., 2025; Hebat & Hidayat, 2026). The persistence of this imbalance suggests that future legal reform should prioritize recognition frameworks capable of connecting digital authentication with legally attributable personhood.

The concept of mutual recognition provides a potential normative foundation for transnational digital identity governance. Comparative examination of the European Union framework demonstrates that legal certainty increases when jurisdictions accept digital identities issued under equivalent regulatory standards rather than requiring repeated verification under domestic procedures. Article 6 of the eIDAS Regulation establishes a recognition obligation grounded in trust, interoperability, and regulatory equivalence, creating a model that extends beyond purely technological cooperation.

Comparative legal reasoning suggests that similar principles could be adapted within broader international frameworks without requiring complete unification of national identity systems. Mutual recognition therefore offers a mechanism through which legal certainty may be strengthened while preserving regulatory autonomy and national sovereignty (Andraško & Mesarčík, 2021). The normative elements of a reconstructed framework may be conceptualized through the following model:

Table 3. Reconstructed Normative Framework for Transnational Digital Identity Recognition and Legal Certainty

Normative Element	Legal Function	Regulatory Objective	Expected Juridical Effect
Mutual Recognition Principle	Recognition of foreign digital identities	Cross-border interoperability	Legal continuity
Equivalence Assessment	Evaluation of regulatory standards	Trust formation	Predictable recognition
Attribution Framework	Identification of legal actors	Accountability	Enforceability
Data Governance Integration	Protection of personal data	Rights protection	Regulatory legitimacy
Dispute Resolution Mechanism	Cross-border adjudication support	Procedural certainty	Effective remedies

The table illustrates that digital identity recognition requires a multidimensional regulatory architecture rather than isolated authentication standards. Each normative element addresses a distinct legal challenge while simultaneously contributing to legal certainty. The relationship between recognition, attribution, and enforceability demonstrates that digital identity should be understood as a foundational legal institution within transnational commerce. Normative coherence emerges only when these elements operate as an integrated framework rather than as independent regulatory mechanisms.

Legal attribution occupies a central position within this reconstructed model because rights and obligations cannot be enforced without a legally identifiable subject. Article 11 of the ITE Law recognizes electronic signatures as instruments capable of authenticating electronic transactions, yet the provision primarily addresses validity rather than transnational recognition. Comparative doctrinal analysis demonstrates that attribution mechanisms must be expanded beyond technical verification to include legal recognition of identity credentials originating from foreign jurisdictions. Research concerning smart contracts and digital assets reveals that anonymity and pseudonymity frequently undermine accountability despite the existence of technologically reliable transaction records (Situmorang & Salam, 2025). A reconstructed framework should therefore require identity systems capable of linking digital actions to legally recognizable actors while preserving proportional privacy protections.

The integration of consumer protection principles constitutes another indispensable component of normative reconstruction. Consumer rights become difficult to enforce where digital identities cannot be verified consistently across borders, particularly in transactions involving foreign marketplaces and decentralized digital services. Studies examining cross-border electronic commerce repeatedly identify identity uncertainty as a significant obstacle to effective legal remedies and dispute resolution mechanisms (Heng & Lie, 2025; Fitriani et al., 2025). Article 4 of the Indonesian Consumer Protection Law guarantees access to information, legal certainty, and fair treatment, values that cannot be fully realized without reliable identification of commercial actors. Normative reconstruction should consequently incorporate mandatory recognition standards capable of strengthening accountability within transnational consumer transactions.

Data protection considerations must be incorporated directly into any framework governing digital identity recognition. Digital identity systems process substantial quantities of personal information, creating risks associated with unauthorized disclosure, surveillance, and regulatory fragmentation. Comparative legal scholarship demonstrates that recognition mechanisms lacking robust data governance safeguards may generate legal uncertainty rather than reducing it because trust depends upon both authenticity and protection of personal rights (Sullivan, 2014; Sharma, 2025). Indonesian regulatory developments concerning personal data protection similarly reflect growing awareness that digital economic participation requires effective safeguards for informational autonomy (Kaplale & Maulana, 2026). The reconstructed framework should therefore integrate recognition and data protection as complementary dimensions of legal legitimacy.

Cross-border enforcement considerations further reinforce the necessity of a coordinated normative architecture. Cybercrime investigations, electronic evidence assessment, and transnational dispute resolution frequently depend upon reliable identification of persons operating across multiple jurisdictions. Comparative studies concerning cybercrime jurisdiction and admissibility of digital evidence indicate that fragmented identity standards often obstruct legal cooperation and weaken enforcement effectiveness (Eswaramoorthi, 2026; Islami, 2025). Article 5 of the ITE Law recognizes electronic information and electronic documents as legal evidence, yet evidentiary reliability remains connected to the ability to verify the identity of the relevant actor. Recognition frameworks capable of supporting attribution across jurisdictions would consequently strengthen both private law enforcement and public regulatory oversight.

Normative reconstruction must also account for ongoing transformations in digital trade governance. Emerging technologies such as distributed ledger systems, electronic transferable records, and decentralized payment infrastructures increasingly operate within transnational commercial networks that transcend conventional jurisdictional boundaries. Legal analyses concerning digital trade modernization emphasize that future commercial systems will depend upon trusted identity infrastructures capable of facilitating recognition across heterogeneous regulatory environments (ALsheyab, 2025; Zetzsche et al., 2021). Comparative scholarship concerning digital transformation similarly suggests that legal paradigms rooted exclusively in territorial assumptions are becoming progressively inadequate for regulating digitally interconnected economies (Taufani & Negara, 2026). Sustainable legal certainty therefore requires normative models capable of adapting to technological evolution without sacrificing accountability and legal predictability.

The reconstructed framework developed through this doctrinal and comparative analysis supports a conception of digital identity as a transnational legal institution grounded in mutual recognition, regulatory equivalence, legal attribution, data protection, and procedural enforceability. International legal instruments, Indonesian legislation, comparative regulatory models, and contemporary legal scholarship collectively indicate that existing approaches remain fragmented despite increasing reliance upon digital commerce and cross-border electronic transactions (Susilowati et al., 2025; Savita et al., 2025; Wulandari et al., 2025). Legal certainty cannot be sustained where identity recognition remains dependent upon isolated domestic standards incapable of producing predictable legal effects beyond national borders. A transnational recognition framework would strengthen contractual validity, evidentiary reliability, consumer protection, and enforcement effectiveness while simultaneously respecting legitimate concerns regarding sovereignty and regulatory diversity. The normative reconstruction proposed in this study consequently contributes to the development of a more coherent legal architecture for digital identity governance within the evolving ecosystem of global electronic commerce (Rahmatullah & Subair, 2024; Toyi & Hamidun, 2025).

CONCLUSION

The analysis confirms that digital identity has evolved beyond its traditional function as a technological authentication mechanism and now operates as a foundational legal institution determining attribution, accountability, and enforceability within cross-border electronic transactions. Existing international and national regulatory frameworks recognize the validity of electronic transactions and electronic signatures, yet they remain fragmented in addressing the legal recognition of digital identities across jurisdictions, creating significant uncertainty concerning contractual validity, evidentiary status, consumer protection, and regulatory enforcement. Comparative examination reveals that the principal challenge lies not in technological interoperability but in the absence of coherent normative mechanisms capable of ensuring continuity of legal identity between different legal systems. Jurisdictional fragmentation, divergent recognition standards, and inconsistent approaches to data governance further weaken legal predictability within transnational digital commerce. A reconstructed framework grounded in mutual recognition, regulatory equivalence, legal attribution, integrated data protection, and effective cross-border enforcement offers a more coherent juridical foundation for digital identity governance. Such a framework strengthens legal certainty by enabling digital identities to receive predictable legal effects across jurisdictions while preserving accountability, protecting individual rights, and supporting the sustainable development of the global digital economy.

REFERENCES

Abhipraya, A. R., Pradana, A. K. A. P., Mahardika, Y. P., Putra, R. T., & Susanto, A. (2025). Perkembangan Hukum Perjanjian di Era Digital: Dari Konvensional ke Elektronik. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, *5*(1), 365-375. https://doi.org/10.56799/peshum.v5i1.12660.

Agusnur, A. (2025). Perlindungan Hukum bagi Konsumen dalam Transaksi Perdagangan Elektronik di Indonesia. *Jurnal Hukum Perdata dan Bisnis*, *1*(1), 1-7.

ALsheyab, M. S. A. (2025). Legal analysis of the merits of electronic transferable records: toward cross-border trade digitalization. *International Journal of Law and Management*, *67*(1), 145-163. https://doi.org/10.1108/IJLMA-09-2023-0209.

Andraško, J., & Mesarčík, M. (2021). Those who shall be identified: The data protection aspects of the legal framework for electronic identification in the European Union. *TalTech Journal of European Studies*, *11*(2), 3-24.

Azam, M., Alwreikat, N. M., Alsyouf, B., Al Fandi, A. S. A. A., & Pharaon, R. A. K. M. (2026). Contemporary Trade Governance and Cross-Border Data Flows: A Comparative Study of Sharīʿah Principles and International Legal Frameworks. *MILRev: Metro Islamic Law Review*, *5*(1), 686-721. https://doi.org/10.32332/milrev.v5i1.13387.

Espinal De Aza, E. L. (2023). Blockchain and the Transformation of the Registry System: Towards a New Model of Digital Legal Certainty. *Available at SSRN 5633470*. https://dx.doi.org/10.2139/ssrn.5633470.

Eswaramoorthi, R. (2026). Cross-Border Cybercrime Jurisdiction and Digital Evidence Admissibility: A Comparative Legal Framework. *Sirashmi Perspectives in Cyber Law, Intellectual Property, and Legal Studies*, 1-19.

Fitriani, I., Maulia, I., & Dafira, L. (2025). Perlindungan Hukum terhadap Konsumen dalam Transaksi E-Commerce Lintas Negara. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *3*(3), 1387-1397. https://doi.org/10.61104/alz.v3i3.1323.

Hebat, I. Y., & Hidayat, A. (2026). The Reform of Electronic Contract Regulations in Indonesia: Strengthening Legal Certainty in Digital Transactions. *Journal of Lex et Justitia*, *2*(2), 1-17. https://doi.org/10.67171/h0qpbq51.

Heng, R. J., & Lie, G. (2025). Perlindungan hukum bagi konsumen dalam transaksi cross-border pada platform marketplace digital berdasarkan hukum positif Indonesia. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *12*(10), 3886-3899. https://doi.org/10.31604/jips.v12i10.2025.3886-3899.

Islami, Z. P. (2025). Tantangan Penegakan Hukum di Era Globalisasi Digital: Strategi Nasional Menghadapi Kejahatan Siber Lintas Batas. *Aksioma: Jurnal Sains Ekonomi dan Edukasi*, *2*(12), 2579-2591. https://doi.org/10.62335/aksioma.v2i12.1985.

Kaplale, M. I., & Maulana, D. (2026). Legal Protection of Personal Data in Indonesia's Digital Ecosystem: Challenges for Regulatory Enforcement and Legal Certainty. *Journal of Lex et Justitia*, *2*(2), 18-32. https://doi.org/10.67171/d1qff634.

Luviana, D., & Pratiwi, S. H. (2026). Perlindungan Konsumen dalam Perdagangan Elektronik Lintas Negara dan Tantangan Digital. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(3), 904-915. https://doi.org/10.61104/alz.v4i3.5354.

Ming-zhe, S., Geng, C., & Hong-wei, W. (2025). Jurisdiction over electronic contracts in cross-border tourism disputes between China and Kazakhstan: Dilemma and path. *BULLETIN of LN Gumilyov Eurasian National University Law Series*, *151*(2), 243-253. https://doi.org/10.32523/2616-6844-2025-151-2-243-253.

Rahmatullah, R., & Subair, L. (2024). Dampak Hukum Terhadap Konsumen Dalam Transaksi E-Commerce Cross–Border. *Jurnal To Ciung: Jurnal Ilmu Hukum*, *4*(2), 17-29. https://doi.org/10.64078/tociung.v4i2.2870.

Savita, S. R., Mahfud, M. A., & NGA, P. T. (2025). Normative fragmentation in Indonesian notary law: Regulatory harmonization of cyber notary and electronic signatures toward structural justice. *Potret Pemikiran*, *29*(2), 282-304. https://dx.doi.org/10.30984/pp.v29i2.4091.

Sharma, A. (2025). Legal Dimensions Of Digital Transformation: A Study On Data Protection And Business Sustainability In The Digital Economy. *International Journal of Business Management & Legal Affairs*, *1*(1), 41-55. https://doi.org/10.65512/41dmtn51.

Situmorang, M. E., & Salam, A. (2025). Analisis Aspek Hukum Kontrak Pintar dalam Transaksi Kebendaan Digital: Tantangan Anonimitas dan Peran Identitas Digital. *Lex Patrimonium*, *4*(1), 2.

Sullivan, C. (2014). Protecting digital identity in the cloud: Regulating cross border data disclosure. *Computer Law & Security Review*, *30*(2), 137-152. https://doi.org/10.1016/j.clsr.2014.01.004.

Sullivan, C. (2018). Digital identity–From emergent legal concept to new reality. *Computer Law & Security Review*, *34*(4), 723-731. https://doi.org/10.1016/j.clsr.2018.05.015.

Susilowati, D. E., Muhtarom, M., & Junaidi, A. (2025). Analisis yuridis keabsahan tanda tangan digital dalam transaksi e-commerce di Indonesia. *Jurnal Penelitian Serambi Hukum*, *18*(01), 17-26. https://doi.org/10.59582/sh.v18i01.1254.

Taufani, G., & Negara, I. P. E. W. (2026). Legal Paradigm Shifts In The Age Of Digital Transformation. *Realism: Law Review*, *4*(1), 54-75. https://doi.org/10.71250/rlr.v4i1.131.

Toyi, A. R., & Hamidun, E. Z. P. (2025). Establishing Legal Certainty in the Digital Era: Challenges and Solutions. *Estudiante Law Journal*, *7*(2), 444-460. https://doi.org/10.33756/eslaj.v7i2.31630.

Utomo, A. P., Ibrohim, N. M., Ramadhani, N., Zidni, N. M., & Wahyuaristy, D. S. (2025). Konsep ideal regulasi identitas digital tunggal dalam konvergensi teknologi sebagai instrumen penguatan perdagangan digital berbasis ekonomi virtual. *Forschungsforum Law Journal*, *2*(02), 119-141. https://doi.org/10.35586/flj.v2i02.11161.

Wulandari, D., Manurung, R. A., Yuscinlica, M. I., & Sari, A. K. (2025). Analisis Hukum Transaksi Digital Lintas Negara Berdasarkan Prinsip Uncitral Model. *Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora*, *3*(4), 113-125.

Zetzsche, D. A., Anker-Sørensen, L., Passador, M. L., & Wehrli, A. (2021). DLT-based enhancement of cross-border payment efficiency–a legal and regulatory perspective. *Law and Financial Markets Review*, *15*(1-2), 70-115. https://doi.org/10.1080/17521440.2022.2065809.