JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(2), 1857-1866
ISSN: 2589-1316

Reconstruction of Notary Authority in Fiscal Compliance Disclosure in the Cyber Notary Era

Edy Gunawan[1], Denock Vindiya Sari[2], Nathanael Abiel[3], Agus Budianto[4]*

[1] *Magister of Law Department, Universitas Pelita Harapan, Jakarta,* INDONESIA
[2] *Magister of Notary Department, Universitas Pelita Harapan, Jakarta,* INDONESIA
[3] *Magister of Law Department, Universitas Pelita Harapan, Jakarta,* INDONESIA
[4] *Magister of Law Department, Universitas Pelita Harapan, Jakarta,* INDONESIA

***Corresponding Author:** agus.budianto@uph.edu

Citation: Gunawan, E., Sari, D. V., Abiel, N. and Budianto, A. (2025). Reconstruction of Notary Authority in Fiscal Compliance Disclosure in the Cyber Notary Era, *Journal of Cultural Analysis and Social Change*, 10(2), 1857-1866. https://doi.org/10 10.64753/jcasc.v10i2.1881

Published: November 15, 2025

ABSTRACT

This research reconstructs the authority of notaries in the era of cyber notary by relating the function of proving authentic deeds to verification of tax compliance of the witnesses. Departing from a normative juridical method supported by limited empirical data, this study combines legislative, conceptual, and comparative approaches to harmonize various relevant regulations. The results of the study show that the probative equality of electronic documents requires strict technical prerequisites—including certified electronic signatures, authoritative time-stamping, tamper-evident trail audits—along with the functional equivalent of attendance, reading, and signing. The integration of NIK-NPWP and risk-based tax KYC protocols strengthens identity accuracy and completeness of fiscal obligations, but must be limited by the principles of privacy-by-design, purpose limitation, and role-based access control. This article proposes a draft of operational standards, deed clauses regarding the disclosure and retention of fiscal data, and an architecture of interoperability between notarial systems, trust services, population, and taxation. Policy implications include strengthening accountability, service efficiency, and legitimacy of evidence, as well as reinforcing the code of ethics and fulfilling the right to data protection in the digital legal ecosystem. Methodologically, the main contribution of this research lies in the integration of dogmatic analysis with technical specifications that can be audited as the basis for policy feasibility tests.

Keywords: Reconstruction, Notary, Authority, Tax Compliance, Cyber Notary

INTRODUCTION

Digital transformation in legal governance is driving a fundamental shift in the way states ensure certainty, order, and justice (Tobing Lumban, 1999). In the midst of this current, the Notary—as openbare ambtenaar—remains the main buffer for the validity of legal acts through authentic deeds (Sesung, 2017). The acceleration of digital transformation is driving the shift of notarization practices from physical processes to service ecosystems that utilize electronic documents and signatures. This change also links notarial services with tax administration, which is increasingly digitized and integrated across administrative databases. This connectivity opens up opportunities to increase legal certainty but at the same time presents normative and operational challenges that are not simple.

In the context of the concept of 'cyber notary', this paper interprets Notary as a public official who carries out the task of proving and legalizing with an electronic medium that meets authentic requirements (Nurita, 2012). The obligation to disclose the tax compliance of the attendees is understood as part of the functions of prudence, risk prevention, and legal counseling inherent in the position (Sari, 2023). The main objective is to

ensure that notarized legal events do not close fiscal obligations and do not cause derivative legal consequences for the parties (Alincia, 2021). Another goal is to strengthen the integrity of the deed making process through identity verification, payment validation, and traceable electronic recording (Lubis, 2023).

The positive legal framework shows the tension between the requirements of physical presence reflected in traditional notary practices and the recognition of electronic documents as valid evidence. These tensions result in the blurring of the boundaries of authority in facilitating online meetings, verifying identities remotely, and placing electronic signatures in an equivalent degree of authenticity. That ambiguity has an impact on the vulnerability of proof if process engineering and electronic records are not prepared to adequate standards. Uncertainty also arises when the formalism of the deed meets technical innovation without a clear procedural umbrella. This condition demands a reconstruction of norms that unite formal and technical aspects in one consistent evidentiary design.

The next problem arises in the intersection between job secrets, access to tax data, and the principle of personal data protection. The need for tax verification presupposes legitimate and proportionate access to the fiscal identity and proof of payment of the beneficiaries. Unregulated access poses a risk of confidentiality violations and potential data misuse leading to disputes or sanctions. The absence of informed consent standards and a testable audit trail undermines process accountability. Therefore, access governance must be based on objective limitation, data minimization, and documented role-based controls.

In addition, challenges also appear at the operational level when digital tools and procedures are not fully aligned with the needs of proof in court. The difference in technical capacity between Notary offices affects the quality of verification, storage security, and the sustainability of electronic archives. The disintegration of the inter-agency administrative system hinders workflows that require quick and precise validation of tax status and population identity. This inequality creates a variety of practices that have the potential to erode the uniformity of professional standards and the equality of the parties before the law. Technical and procedural harmonization is a requirement so that digital innovation does not lead to service disparities. In the context of cyber notaries which combine tax compliance verification, position secrecy, and personal data protection, there is no measurable operational model—risk-based, audit trail, and NIK-NPWP interoperability—that can be used as notarial SOPs to integrate tax compliance disclosure into the electronic deed workflow.

The problem statement in this article covers the limits and configuration of the Notary's authority in revealing the taxation aspects of clients in the electronic service ecosystem. The next formulation targets how a procedural integration model ensures the validity of evidence, fiscal compliance, and data protection simultaneously. The purpose of this article is to develop a normative and operational construct that balances verification accuracy, process traceability, tax compliance, and professional ethics.

METHOD

This article uses a normative juridical method with limited empirical data support (Negara, 2023). The main focus is to examine the legal norms that govern the position of notary, electronic proof, access and disclosure of tax data, and personal data protection. The approaches used include a statute approach to interpret and harmonize laws and regulations, a conceptual approach to build a work definition related to cyber notary and electronic authentic deeds, and a comparative approach to examine practices in various civil law and common law jurisdictions. The analysis was carried out qualitative-prescriptive through norm mapping, regulatory content analysis, and pattern matching between legal provisions and field practice. Validity is strengthened through triangulation across legal sources and methods, while reliability is maintained through documented analytical trail audits. The ethical aspect is guaranteed through informant consent, restrictions on the purpose of data use, and the elimination of personal identity. Thus, this methodology is able to produce a balanced, auditable, and relevant normative and operational construction to build a ius constituendum regarding notary obligations in disclosing tax compliance in the cyber notary era.

RESULT AND DISCUSSION

Reconstruction of Notary Authority in the Cyber Notary Era

The configuration of notary authority initially came from the attribution of the law that placed the notary as the general official of making authentic deeds (Zamili, 2022). The attribution is attached to three main pillars, namely material authority over the type of legal act, personal authority over the subject served, and territorial authority over the place of service. The power of proving an authentic deed rests on the fulfillment of the requirements for form, presence, and procedures set by laws and regulations. In that framework, the role of the notary is not just the "author" of the deed, but the guardian of the order of private proof that has public

implications (Laksana, 2019). The shift towards digital services requires a rereading of the attribution to be compatible with electronic media without reducing the authenticity of the deed.

General attribution requires technology to be operationalized in the digital ecosystem. The technicality includes standardization of the identification of the parties, process recording mechanisms, and how to ratify signatures on electronic media (Hutapea, 2023). Without adequate technical arrangements, attribution power risks being practiced inuniformly, resulting in disparities in probative value. General rules should be translated into auditable work parameters, such as trail audit requirements, reliable timestamps, and document verification codes. Thus, the boundaries of authority remain firm even though the means of implementation have changed.

The recognition of information and electronic documents as legal evidence has shifted the evidentiary landscape that has been centered on paper documents. Electronic signatures that meet certain qualifications reinforce the principle of non-repudiation and allow for remote execution of agreements (Gregušová, 2022). This shift requires a reconciliation between the principle of deed formalism and flexible and programmatic digital characters. The principles of lex specialis and lex posterior need to be harmonized so that there is no conflict of application between the notary legal regime and the electronic proof regime. The harmonization ensures that equivalence is not only recognized normatively, but also forensically proven when tested in court.

The equivalence of electronic evidence with an authentic deed is not born automatically, but requires the fulfillment of strict and documented procedural prerequisites. Technical standards such as signer identity certification, securing file integrity through hash chaining, and time assurance through time-stamping authority need to be instituted as default notarial protocols and not just optional best practices (Lubis, 2022). Without this foundation, the "electronic" status would turn into a cosmetic label that could not prevent manipulation, identity spoofing, and document splicing that undermined authentic value (Putri, 2019). A reliable normative framework demands coherence between the definition of the deed, the procedure for making it, and the criteria for electronic evidence, so that each element of the process corroborates each other in a chain of evidence (Monaghan, 2022). The validity of deeds no longer depends on physical materials, but on the quality of governance inherent in the life cycle of digital documents.

The formal implications of an authentic deed touch on three critical nodes—the presence of the parties, the reading of the deed, and the signing—each of which demands a functional equivalent in the digital space. An online presence requires multi-layered verification that goes beyond visible observation and creates an in-depth defense against the risks of identity disguise, coercion, and collusion. Reliable credential analysis must be combined with liveness detection, proportionate biometric checks, and knowledge-based authentication tailored to the risk profile of the person facing and the type of legal act notarized (Bungdiana, 2023). All interaction sessions, including the reading and approval processes, need to be continuously recorded, assigned a unique session ID, and linked to an electronic minuta through a verifiable seal that binds content and context. Witnesses and officials are required to carry out documented cross-control roles, so that human oversight remains present as an ethical and procedural safeguard above system automation (Ni'mah Sona, 2022).

Tax compliance verification should only be carried out as long as it is necessary for the validity of notarized legal actions, so that it does not turn into a fishing expedition that exceeds the requirements of the deed. Any access to fiscal data must be recorded in an intact, auditable event-driven log that shows who accessed what, when, for what purpose, and with what verification results (Kutyłowski, 2023). The preparation of comprehensive derivative regulations must integrate the formal requirements of deeds, trust services standards, and electronic proof mechanisms in one consistent procedural design across regimes. Detailed operational guidelines need to establish clear roles, responsibilities, escalation paths, and reporting pathways to prevent compliance gaps and regulatory arbitrage (Fang, 2020). Inter-agency coordination—between notary authorities, population administration, taxation, and data protection—is key to identity integration and fiscal verification as a seamless workflow (Noviana, 2012). With this approach, change is no longer patchy, but rather results in an end-to-end architecture that is integrated from upstream to downstream.

Harmonization between regulations needs to be complemented by measurable and auditable minimum technical standards, so that enforcement does not depend solely on casuistic interpretation. These standards include, among others, secure cryptographic key management, granular role-based access control, proportional record retention policies, geo-redundant backups, and regularly tested disaster recovery plans. Certification for trusted service providers, electronic signature providers, and digital archive managers should be linked to incident reporting, penetration testing, and vulnerability disclosure program requirements to ensure readiness in the face of threats.

In addition, professional organizations need to adopt a code of practice that clarifies ethical expectations in the digital context, including prohibitions on practices that obscure presence, manipulate records, or over-collect data. Effective oversight requires measurable compliance performance indicators, internal control dashboards, and feedback mechanisms that can trigger continuous improvement.

It can be drawn a common thread that the reconstruction of authority is not enough to be done at the norm level, but must be accompanied by strengthening institutional capacity and adequate technological literacy at the operator level. Ongoing training programs need to combine procedural law and evidentiary techniques with aspects of information security, risk management, and data processing ethics, so that officials and staff understand the why, what, and how of each procedural step. Investment in trusted infrastructure—including reliable recording devices, secure vaulting, and key management systems—needs to be encouraged through incentive schemes, technical cooperation, and credible accreditation. Periodic evaluation of the implementation of digital procedures, both through internal audit and external conformity assessment, will produce data-based feedback that is useful for improving regulations and SOPs. With this series of steps, notary authority in the cyber notary era is not only compatible with technology, but also remains faithful to its constitutional mission—maintaining legal certainty, protecting the rights of parties, and supporting the reliability of proof in the digital economy.

Integration of Identity of Population and Taxation in Notarial Services

The integration of the Population Identification Number (NIK) and the Taxpayer Identification Number (NPWP) lays the foundation of a dual identity that strengthens each other so that the civil profile and fiscal profile of the attendees can be verified consistently in one administrative and legal ecosystem (Amila, 2023). This linkage allows notaries to test the suitability of personal data, tax subject status, and formal compliance records without separating the identification process from the assessment of tax obligations relevant to legal events. The alignment of population and taxation databases also reduces the risk of impersonation, identity switching, and the use of unauthorized identity attributes in transactions that have significant fiscal consequences. At the evidentiary level, identity integration strengthens the reliability of the deed because each statement of the parties can be linked to an identity that has been verified across authorities. Thus, the NIK-NPWP functions as an anchor of trust that balances legal certainty, administrative efficiency, and accountability of electronic proof.

From an operational perspective, the integration translates into a multi-layered verification flow that combines real-time or near-real-time checking of demographic data, taxpayer status, and arrears flags to prevent false acceptance or rejection (Schreiner, 1999). Notaries organize a pre-screening process that tests the identity match between the population document and the tax record, then ties the results to the case profile and the type of deed to be issued. The verification results are stored as an event record that can be audited and linked to electronic minutes through a unique marker that prevents falsification or disconnection of evidence. This approach provides adequate traceability without compromising the principle of data minimization as only attributes relevant to the deed are processed and stored (Cao, 2023). The final effect is a risk-aware, measurable, and proportionate notarial work arrangement to the purpose of proof.

The notarial tax Know Your Customer protocol is designed to orchestrate identification, validation, and recording so that all risk nodes can be controlled systematically and documented. The identification stage establishes the certainty of the identity of the attendees by relying on valid proof of residency and, where necessary, the reinforcement of two-factor authentication that considers the value and complexity of the transaction. The validation stage examines relevant fiscal attributes, including the status of the tax subject, the provisions of the applicable tax regime, and evidence of the fulfillment of payment or reporting obligations that are prerequisites for legal events. The recording stage builds an electronic chain of custody that binds identities, examination (Burri, 2020) results, and evidence attachments so that they remain intact throughout the life cycle of the deed.

The implementation of tax KYC in practice requires a risk-based approach that differentiates the intensity of checks according to transaction profiles, compliance records, and anomalous indicators detected. For cases of high value, cross-jurisdictional, or involving multi-layered ownership structures, enhanced due diligence is enabled to ensure that the source of funds, object of transaction, and fiscal consequences have been adequately tested (Gaviyau, 2023). Each step of the audit is tied to a trail audit that records the perpetrators, timing, system, and results, so that a reconstruction of the process can be carried out if a proof dispute arises at a later date. Record retention is structured with policies that balance the need for proof and data protection, including strict access control mechanisms to avoid function creep (Koops, 2021).

The deed clause on tax compliance is designed as a transparency instrument that affirms the scope, legal basis, and legal consequences of the parties' statements regarding the status and fulfillment of fiscal obligations. The clause should state that tax data is processed for the specific purpose of making the deed in question, with limitations on relevant attributes, and with a proportionate and accountable retention period. The series of statements of the parties contains confirmation of the correctness of the data, the suitability of supporting documents, and an understanding of the civil and administrative consequences in the event of untruthfulness or

obscuration of material facts. The notary binds the attachment of the proof of payment or receipt transaction number explicitly as an integral part of the minuta, so that the continuity of the evidence is maintained.

At the same time, the clause needs to provide clear allocations of risk without going beyond the limits of the profession's authority, by distinguishing between the notary's fair verification obligations and the substantive responsibilities of the parties to their data and tax obligations. The structure of the clause may include representations and warranties regarding fiscal status, undertakings to submit additional documents when requested by the authority, as well as acknowledgements about the processing of data that have been described at the time of consent. Notaries may add a limited disclaimer asserting that substantive tax assessments remain with the fiscal authority, while notarial verification is formal and procedural to maintain evidentiary certainty.

There are several cases of transfer of land and/or building rights that illustrate how the integration of identity and taxation shortens service time while thickening administrative certainty. The workflow begins with matching the identities of the parties to the population database, followed by mapping final income tax and BPHTB obligations based on the characteristics of the object and the agreed transaction value. The notary then facilitates the issuance of billing and verification of the State Revenue Transaction Number linked to the minuta as an electronic attachment with a unique marker. After the proof of fulfillment of the obligation is verified and recorded, then the deed is read and signed with an electronic signature mechanism that meets the non-repudiation. This series of steps provides end-to-end traceability that facilitates auditing, correction, and law enforcement in the event of a dispute.

In the case of a closed limited liability company's share transfer, identity and tax integration helps control the risk of nominee arrangements, hidden (Kusuma, 2022) beneficial ownership, (Meunier, 2018) and under-reporting of transaction values (Jenkins, 2018). The verification stage assesses the fiscal status of the parties and related legal entities, then maps the implications of income tax on transfer and the potential for VAT depending on the nature of the object and business activity. The notary ensures the conformity of the transfer data with the last cap table, articles of association, and approval of the company's organs, as well as linking financial proof documents as validated attachments. If the transaction involves cross-border flows, (Chin, 2022) the notary adds procedural records regarding withholding, treaty relief, (Shehaj , 2022) or the need for transaction reports in accordance with the provisions of laws and regulations.

The first technical challenge that must be answered is the interoperability of the system between the application of the notary's office, trust services, and the infrastructure of population administration and taxation. Interoperability requires documented interface specifications, stable message formats, and data exchange governance that governs quality, error handling, and service-level objectives. Without a harmonized architecture, any verification process is at risk of latency, data mismatch, (O'Reilly, 2021) or failures that degrade efficiency and damage the experience for parties. The use of federated identities that map NIK to NPWP and other fiscal attributes accelerates cross-checks while maintaining data sovereignty in each authority. This design prevents vendor lock-in and allows for technology evolution without compromising procedural certainty.

The second technical challenge concerns robust audit trail design, data leak control, and resilience to cybersecurity incidents in the context of electronic proof. The audit trail must be tamper-evident, contain the identity of the perpetrator, an authoritative timeline, and a sufficient summary of actions to reconstruct the process without over-exposing sensitive data. Role-based access control, encryption in transit and at rest, and continuous anomaly monitoring become non-negotiable layers of control. When an incident occurs, a tested incident response plan—from containment, forensic preservation, to notification to the right party—determines the reputation and legitimacy of digital notary services. With such a governance tool, the integration of identity and taxation in the realm of notary is not only possible, but also reliable and legally accountable.

Privacy Governance, Electronic Evidence, and Standardization of Practice

The application of the principle of privacy-by-design in cyber notary practice means that the mechanism for protecting personal data is not placed as an additional element, (Alkhariji, 2023) but is embedded from the stage of designing electronic notary systems, procedures, and applications (Aljeraisy, 2022). This concept ensures that every function—from party authentication, document storage, to recording online court proceedings—always minimizes data collection, limits processing to specific purposes, and involves proportionate access control (Barth, 2023). The principle of purpose limitation also strengthens the framework by emphasizing that fiscal and population data used in the deed process should only be processed for the purpose of creating authentic deeds, without paving the way for other functions outside the mandate of the position. The integration of these two principles allows for a balance between legal certainty, transaction security, and the protection of the fundamental right to privacy of the parties.

In the operational framework, privacy-by-design is realized through default privacy settings policies (Uribe, 2020), data encryption at every stage of the workflow, and separation of access authority between notary

officials, administrative staff, and technology service providers. Any requests for access to data must be recorded in an event-driven audit log that automatically flags who accessed (Corrales, 2022) when, and for what purpose, allowing for process reconstruction in the event of a dispute or violation. The application of this principle reduces the risk of function creep—i.e., the use of data for inappropriate purposes—and ensures that sensitive data remains under the control of legitimate institutions. Furthermore, purpose limitation binds officials to communicate information transparently to the parties about how their data is used, stored, and at what point it will be deleted (Nicole, 2021).

The probative value of electronic evidence in the context of cyber notary rests on three main instruments: certified electronic signatures, time-stamping, and tamper-evident records. Certified electronic signatures guarantee a direct link between the signer and the document, so it is impossible to deny or reject it in the future. Time-stamping performed by a trusted authority ensures that each legal action is recorded in a chronological order that cannot be manipulated, closing the space for disputes regarding the timing of the will statement. Meanwhile, tamper-evident records maintain the integrity of documents by creating an instant detection mechanism in case of changes to the deed text or evidence attachments. The combination of these three instruments gives electronic evidence the status equivalent of a traditional authentic deed, as long as all procedures are carried out in accordance with applicable legal standards.

In practice, the effectiveness of electronic evidence is highly dependent on the existence of an officially accredited trust guarantee institution that is subject to international standards (Januar, 2020). The process of signature certification, time endorsement, and track record verification must be managed by a party with technical capabilities and legal integrity. Every transaction record needs to be tied to an unbreakable chain of custody, so that interested parties can trace their validity from start to finish. Without this mechanism, electronic evidence is vulnerable to being contested in litigation and losing its authentic force. Therefore, the integration of probative technology into notarial governance is not an option, but rather a prerequisite for digital transformation to produce the same legal certainty as conventional practices.

International standards such as ISO/IEC 27001 on information security management (Culot, 2021), ISO/IEC 27701 on privacy, and the ETSI EN 319 framework for trust services provide a reference that can be adopted in the Indonesian cyber notary system. This standard provides measurable parameters related to encryption, auditing, risk management, and adequate data governance to close security gaps (Shivam, 2022). In addition, the NIST SP 800-63 guideline on digital identity (Burr, 2006), provides a relevant risk-based authentication framework for face-to-face verification in online deeds (Alhirabi, 2023). The application of these international standards ensures that electronic certificates are not only normatively valid, but also technically robust in the face of cyber threats.

The relevance of international standards for practices in the country lies in their ability to bridge the gap between national regulations, which tend to be descriptive, and highly specific technical requirements. The adoption of these standards can be used as a basis for drafting ministerial regulations or authority regulations that set minimum benchmarks for information security management in notary offices. Thus, notaries are not left to interpret for themselves what is meant by "adequate protection," but rather work within a clear and auditable set of specifications. This will increase the predictability, uniformity, and professionalism of electronic notarial services.

Comparisons with international practice show that remote online notarization in the United States emphasizes procedural validity through multi-factor authentication, audio-visual recording, and electronic attestation that is recognized as equivalent to a physical deed (Alkatiri, 2023). Meanwhile, the European Union through the eIDAS Regulation prioritizes cross-country integration by standardizing trust services, advanced electronic signatures, and qualified trust services that are binding across jurisdictions (Alonso, 2020). Both models demonstrate the importance of striking a balance between legal certainty, technical security, and procedural flexibility in the cyber notary framework. This comparative study shows that the success of notarial digitization depends on coherence between substantive law, formal procedures, and technological infrastructure.

However, differences in social and legal contexts, particularly in Indonesia, and technological capacity require more than simply copying foreign models; they must be adapted to domestic needs. The practice of remote notarization in the US was born within the framework of common law, which differs from Indonesia's civil law, while eIDAS operates within the European Union's integration system, which is not identical to the national institutional configuration. Selective adaptation is necessary, for example, combining US-style online authentication disciplines with EU-style qualified trust services, while maintaining the formalism of deeds required by the Notary Profession Law. In this way, Indonesia can produce a unique hybrid cyber notary model that is legally valid nationally and compatible with global practices.

The challenge of regulatory harmonization is a crucial issue because currently the norms governing notary, data protection, taxation, and electronic transactions are spread across various sectoral laws and regulations that are not fully synchronized. This inconsistency creates the potential for conflict of norms, gray space, and non-

uniform practices between notaries and agencies. Therefore, it is necessary to prepare a uniform, clear, and binding national SOPs, so that each notary office has standard guidelines in operationalizing the principles of privacy-by-design (Uribe, 2020), management of electronic evidence, and integration with the tax and population system. This SOP will not only strengthen predictability and uniformity of practice, but also increase public trust in electronic deeds (Saura, 2022).

Finally, the drafting of a uniform national SOP should involve multi-stakeholder collaboration, including notary professional organizations, regulatory authorities, and technology providers, to ensure that policy documents are not only theoretical, but also realistic in implementation. The SOP needs to regulate in detail the procedures for authentication, approval, recording, storage, as well as procedures for controlling security incidents and reporting compliance. Consistent implementation of this SOP will strengthen the legitimacy of cyber notaries and reduce reliance on individual interpretations that are vulnerable to legal uncertainty. With comprehensive governance, the practice of electronic notarity in Indonesia can be transformed into a modern legal instrument that is accountable, secure, and equivalent to international standards.

Conclusion

The reconstruction of notarial authority in the era of cyber notaries must be based on coherence between norms, procedures, and trust infrastructure, so that digital authentic deeds have probative value equivalent to conventional practices. Such equality is not sufficiently guaranteed by normative recognition of electronic documents, but requires strict technical prerequisites—including certified electronic signatures, authoritative time-stamping, and tamper-evident audit trails—which are institutionalized as an inherent part of notarial practice. At the same time, the doctrine of professional ethics and the principle of personal data protection must inform every stage of the process through the application of privacy-by-design, purpose limitation, and role-based access control, so that tax compliance verification does not shift into a violation of the principle of confidentiality. Within the framework of positive law, the principle of notarial prudence must be understood as the embodiment of public office responsibility that functions as a gatekeeper for the validity of legal actions. This function is carried out proportionally: by ensuring the accuracy of the parties' identities, the completeness of the associated fiscal obligations, and the traceability of the deed process, without exceeding the limits of authority as determined by law. Thus, the principles of legal certainty, accountability, and legitimacy of evidence can be consistently upheld in the digital legal ecosystem.

The practical implications of this idea require a clear, uniform, and auditable operational design. This includes integrating NIK–NPWP to link civil and fiscal profiles, implementing a systematically documented risk-based tax KYC protocol, and establishing minimum information security standards in line with international practices. At the technical level, uniform national SOPs are needed to ensure the compatibility of presence, reading, and signing functions in the digital space; the formulation of deed clauses related to fiscal data disclosure and retention; and the establishment of measurable escalation paths and incident reporting systems. Interoperability between systems—including notary offices, trust services, population administration, and taxation—must be ensured through open interface specifications, measurable service-level objectives, and data exchange governance that prevents vendor lock-in. In addition, strengthening institutional capacity is an important prerequisite, including a continuous training curriculum, accreditation of trusted service providers, periodic security tests, and a transparent tax compliance performance assessment mechanism. Thus, the ius constituendum agenda requires close harmonization between the UUJN, the ITE Law, tax law, and the Personal Data Protection Law, so as to create a mutually reinforcing and consistent regulatory regime.

Acknowledgements

This scientific work is the result of research funded by the LPPM (Institute for Research and Community Service) of Pelita Harapan University through No. 195/LPPM -UPH/VII/2025, dated July 1, 2025, and listed in the Rector's Decree No. 110/SKR-UPH/VII/2025 dated July 1, 2025.

REFERENCES

Alhirabi, et., all. (2023). "PARROT: Interactive Privacy-Aware Internet of Things Application Design Tool." Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 7(1). 1-37. https://doi.org/10.1145/3580880

Alincia, Devi, and Sitabuana, Tundjung. (2021). "Urgency of Law Amendment as Foundation of The Implementation of Cyber Notary." Law Reform: Jurnal Pembaharuan Hukum 17(2). 214-231. https://doi.org/10.14710/lr.v17i2.41749.

Aljeraisy, Atheer, Masoud Barati, Omer Rana, dan Charith Perera. (2022). "Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective." ACM Computing Surveys, 54(5). 1-38. https://doi.org/10.1145/3450965.

Alkatiri, et., all. (2023). "A Legal Perspective: Implementing an Electronic Notarization System in Indonesia in the Post-Pandemic Era." Jambura Law Review 5(2). 332-355. https://doi.org/10.33756/jlr.v5i2.19221.

Alkhariji, Lamya, Suparna De, Rana, and Perera, Charith. (2023). "Semantics-based privacy by design for Internet of Things applications." Future Generation Computer Systems, 138. 280-295. https://doi.org/10.1016/j.future.2022.08.013.

Alonso, Álvaro, Alejandro Pozo, Aldo Gordillo, Sonsoles López-Pernas, Andrés Munoz-Arcentales, Lourdes Marco, dan Enrique Barra. (2020). "Enhancing university services by extending the eIDAS European specification with academic attributes." Sustainability (Switzerland) 12(3). 1-19. https://doi.org/10.3390/su12030770.

Amila, Rizka, and Resi Ariyasa Qadri. (2023). "NPWP vs NIK: Integrating the Single Identity Number in Taxation." Journal of Social Entrepreneurship Theory and Practice 2(2). 76-87. https://doi.org/10.31098/jsetp.v2i2.2054.

Andraško, Jozef, dan Matúš Mesarčík. (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) 1-24. https://doi.org/10.2478/bjes-2021-0012.

Barth, Susanne, Dan Ionita, dan Pieter Hartel. (2023). "Understanding Online Privacy - A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines." ACM Computing Surveys 55(3) 63:1-63.37. https://doi.org/10.1145/3502288.

Bungdiana, Desy, and Arsin Lukman. (2023). "Efektivitas Penerapan Cyber Notary Dengan Meningkatkan Kualitas Pelayanan Notaris Pada Era Digital." JISIP (Jurnal Ilmu Sosial dan Pendidikan) 7(1) 309-318. https://doi.org/10.58258/jisip.v7i1.4216.

Burr, William E., Donna F. Dodson, and W. Timothy Polk. (2006). "NIST SP 800-63 Version 1.0.2, Electronic Authentication Guideline." National Institute of Standards and Technology.

Burri, Xavier, Eoghan Casey, Timothy Bollé, and David Olivier Jaquet-Chiffelle. (2020). "Chronological independently verifiable electronic chain of custody ledger using blockchain technology." Forensic Science International: Digital Investigation 33. https://doi.org/10.1016/j.fsidi.2020.300976.

Cao, Lifeng, Shoucai Zhao, Zhen Sheng Gao, and Xuehui Du. (2023). "Cross-chain data traceability mechanism for cross-domain access." Journal of Supercomputing 79(5). https://doi.org/10.1007/s11227-022-04793-w.

Chastra, Denny Fernaldi. (2021). "Kepastian Hukum Cyber Notary Dalam Kaidah Pembuatan Akta Autentik Oleh Notaris Berdasarkan Undang-Undang Jabatan Notaris." Indonesian Notary 3(2) 248–267. https://scholarhub.ui.ac.id/notary/vol3/iss2/17

Chin, Yik Chan, and Jingwu Zhao. (2022). "Governing Cross-Border Data Flows: International Trade Agreements and Their Limits." Laws 11(4) 1-22. https://doi.org/10.3390/laws11040063.

Corrales Compagnucci, Marcelo, Mark Fenwick, Helena Haapio, and Erik P.M. Vermeulen. (2022). "Integrating law, technology, and design: teaching data protection and privacy law in a digital age." International Data Privacy Law, 12(3) 239-252. https://doi.org/10.1093/idpl/ipac012.

Culot, Giovanna, Guido Nassimbeni, Matteo Podrecca, and Marco Sartor. (2021) "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda." TQM Journal, 33(7) 76-105. https://doi.org/10.1108/TQM-09-2020-0202.

Fang, Weidong, Wei Chen, Wuxiong Zhang, Jun Pei, Weiwei Gao, and Guohui Wang. (2020). "Digital signature scheme for information non-repudiation in blockchain: a state of the art review." Eurasip Journal on Wireless Communications and Networking, 56, 2-15. https://doi.org/10.1186/s13638-020-01665-w.

Gaviyau, William, and Athenia Bongani Sibindi. (2023) "Anti-money laundering and customer due diligence: empirical evidence from South Africa." Journal of Money Laundering Control, 26(7), 224-238. https://doi.org/10.1108/JMLC-06-2023-0103.

Gregušová, Daniela, Zuzana Halásová, and Tomáš Peráček. (2022). "eIDAS Regulation and Its Impact on National Legislation: The Case of the Slovak Republic." Administrative Sciences 12(4), 187. 4-18. https://doi.org/10.3390/admsci12040187.

Hutapea, Christine Willyam, Rahmida Erliyani, and Anang Shophan Tornado. (2023). "Konsep Menghadap Notaris Dalam Pembuatan Akta Berdasarkan Perkembangan Cyber Notary." Collegium Studiosum Journal 6(1) 132–45. https://doi.org/10.56301/csj.v6i1.823.

Januar Wilyana, Rezy, Imam Budi Santoso, and Oci Senjaya. (2020). "Hambatan Dalam Pembuktian Bukti Elektronik Di Persidangan" Singaperbangsa Law Review (SILREV) 1(1). https://doi.org/10.35706/silrev.v1i1.4244.

Jenkins, Matthew. (2018). "Corruption risks in tax administration, external audits and national statistics." Transparency International Anti-Corruption Helpdesk, 2018.

Koops, Bert Jaap. (2021). "The concept of function creep." Law, Innovation and Technology 13(1). 29-56. https://doi.org/10.1080/17579961.2021.1898299.

Kusuma, Andy Putra. (2022). "Nominee Arrangement Practices Performed by The Government of The Republic of Indonesia." Jurnal Hukum Volkgeist 6(2) 196-203. https://doi.org/10.35326/volkgeist.v6i2.2291.

Kutyłowski, Mirosław, and Przemysław Błaśkiewicz. (2023). "Advanced Electronic Signatures and eIDAS – Analysis of the Concept." Computer Standards and Interfaces 83. https://doi.org/10.1016/j.csi.2022.103644.

Laksana, I Putu Gunartha Adi, and Ni Made Ari Yuliarti Griadhi Griadhi. (2019). "Kedudukan Notaris sebagai Membuat Akta dalam Bidang Pertanahan." Kertha Negara 7(11). https://jurnal.harianregional.com/kerthanegara/full-55031

Lim, Chun Yee, Corey Markus, and Tze Ping Loh. (2021). "Precision verification: Effect of experiment design on false acceptance and false rejection rates." American Journal of Clinical Pathology 156(6). https://doi.org/10.1093/ajcp/aqab049.

López Jiménez, David, Eduardo Carlos Dittmar, and Jenny Patricia Vargas Portillo. (2022). "The trusted third party or digital notary in Spain: effect on virtual transactions." International Review of Law, Computers & Technology 36(3): 453–69. https://doi.org/10.1080/13600869.2021.2004760.

Lubis, Ikhsan, Tarsisius Murwadji, Sunarmi, and Detania Sukarja. (2023). "Cyber Notary as A Mean of Indonesian Economic Law Development." Sriwijaya Law Review 7(1): 62-72. https://doi.org/10.28946/slrev.Vol7.Iss1.1972.pp62-72.

Lubis, Ikhsan, Tarsisius Murwadji, Sunarmi Sunarmi, Detania Sukarja, T. Keizerina Devi Azwar, and Faradillah Sitepu. (2022). "Development of the Concept of Cyber Notary in Common Law and Civil Law Systems." Law and Humanities Quarterly Reviews 1(4): 30-39. https://doi.org/10.31014/aior.1996.01.04.32.

Lubis, Ikhsan, Taufik Siregar, and Duma Indah Sari Lubis. (2023). "The Principle of Tabellionis Officium Fideliter Exercebo Related To Cyber Notary." Cognizance Journal of Multidisciplinary Studies 3(6): 422–33. https://doi.org/10.47760/cognizance.2023.v03i06.028.

Mason, Stephen. (2018). "Documents signed or executed with electronic signatures in English law." Computer Law & Security Review 34(4): 933–45. https://doi.org/10.1016/j.clsr.2018.05.023.

Meunier, Denis. (2018). "Hidden Beneficial Ownership and Control: Canada as a Pawn in the Global Game of Money Laundering." SSRN Electronic Journal,. https://doi.org/10.2139/ssrn.3246098.

Monaghan, Nicola. (2022). "Electronic Evidence and Electronic Signatures." Amicus Curiae 3(2): 375-380. https://doi.org/10.14296/ac.v3i2.5418.

Monetery, Fabela Rahma, and Budi Santoso. (2023). "Keabsahan Dan Kekuatan Pembuktian Akta Notaris: Perspektif Cyber Notary Di Indonesia." Notarius 16(2): 666-685. https://doi.org/10.14710/nts.v16i2.41120.

Negara, Tunggul Ansari Setia. (2023). "Normative Legal Research in Indonesia: Its Originis and Approaches." Audito Comparative Law Journal (ACLJ) 4(1): 1–9. https://doi.org/10.22219/aclj.v4i1.24855.

Ni'mah Sona, Mahfuzatun. (2022). "Penerapan Cyber Notary Di Indonesia Dan Kedudukan Hukum Akta Notaris Yang Bebasis Cyber Notary." Jurnal Officium Notarium 2(3): 497-505. https://doi.org/10.20885/jon.vol2.iss3.art12.

Nicole, Olsenn. (2021). Implementing Privacy By Design. Webpage.

Noviana, Ninik. (2012). A Comparison of Notary Powers and Duties in Indonesia, Singapore, and Japan: In Challenges of Law and Governance in Indonesia in the Disruptive Era I.

Nurita, Emma R.A. (2012). Cyber Notary Pemahaman Awal dalam Konsep Pemikiran. Hukum Notaris.

O'Reilly, Jamie A., and Thanate Angsuwatanakul. (2021). "More evidence for a long-latency mismatch response in urethane-anaesthetised mice." Hearing Research 408. https://doi.org/10.1016/j.heares.2021.108296.

Pratama, Iqbal Putra, Fifiana Wisnaeni, and Irma Cahyaningtyas. (2021). "Tanggung Jawab Notaris Terhadap Kewajibannya Dalam Hal Pembacaan Akta." Notarius 14(2):809-817. https://doi.org/10.14710/nts.v14i2.43806.

Putri, Cyndiarnis Cahyaning, and Abdul Rachmad Budiono. (2019). "Konseptualisasi dan Peluang Cyber Notary dalam Hukum." Jurnal Ilmiah Pendidikan Pancasila dan Kewarganegaraan 4(1): 29-42. https://doi.org/10.17977/um019v4i1p29-36.

Rasslan, Mohamed, Mahmoud M. Nasreldin, Doaa Abdelrahman, Aya Elshobaky, and Heba Aslan. (2024). "Networking and cryptography library with a non-repudiation flavor for blockchain." Journal of Computer Virology and Hacking Techniques 20(1): 1-14. https://doi.org/10.1007/s11416-023-00482-1.

Risky, Saiful, Sholahuddin Al-Fatih, and Mabarroh Azizah. (2023). "Political Configuration of Electoral System Law in Indonesia from State Administration Perspective." Volksgeist: Jurnal Ilmu Hukum dan Konstitusi, 30 119–130. https://doi.org/10.24090/volksgeist.v6i1.7940.

Sari, Eka Suci Indria, Rohaini, and Dwi Rimadona. (2023). "Islamic Inheritance Law Review in Notary Practices in Indonesia." Proceedings of the 3rd Universitas Lampung International Conference on Social Sciences (ULICoSS 2022). https://doi.org/10.2991/978-2-38476-046-6_112.

Saura, Jose Ramon, Domingo Ribeiro-Soriano, and Daniel Palacios-Marqués. (2022). "Assessing behavioral data science privacy issues in government artificial intelligence deployment." Government Information Quarterly 39(4). https://doi.org/10.1016/j.giq.2022.101679.

Schreiner, Mark. (1999). A Scoring Model of the Risk of Costly Arrears at a Microfinance Lender in Bolivia. Microfinance Risk Management and Center for Social Development.

Sesung, Rusdianto, Fayakundia Putra Sufi, Roosalina Kartini, and Jeffry Tanugraha. (2017). Hukum dan Politik Hukum Jabatan Notaris. RA De Rozarie, Surabaya.

Sharif, Amir, Matteo Ranzi, Roberto Carbone, Giada Sciarretta, Francesco Antonio Marino, and Silvio Ranise. (2022). "The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes." Applied Sciences (Switzerland). https://doi.org/10.3390/app122412679.

Shehaj, Pranvera. (2022). "Withholding taxes in developing countries: Relief method and Tax sparing in tax treaties with OECD members." SSRN Electronic Journal, https://doi.org/10.2139/ssrn.4184615.

Shivam Kamlesh Mishra. (2022). "Study on Digital-Signatures and Remote Online Notarization." International Journal of Advanced Research in Science, Communication and Technology. https://doi.org/10.48175/ijarsct-5408.

Tobing Lumban, G.H.S. (1999). Peraturan Jabatan Notaris. Erlangga.

Uribe, Daniel. "Privacy Laws, Non-Fungible Tokens, and Genomics. (2020). " The Journal of The British Blockchain Association 3(2). https://doi.org/10.31585/jbba-3-2-(5)2020.

Uribe, Daniel, Gisele Waters, and Genobank Io. (2020). "Privacy Laws, Genomic Data and Non-Fungible Tokens." The Journal of The British Blockchain Association 3(2): 1-10. http://10.31585/jbba-3-2-(5)2020

Zamili, Mavoarota Abraham Hoegelstravores. (2022). "Analisis Yuridis Tentang Kewajiban Notaris Menerapkan Prinsip Mengenali Pemilik Manfaat (Beneficial Ownership) Dalam Proses Pembuatan Akta Badan Hukum Perseroan Terbatas." Fiat Iustitia : Jurnal Hukum, 2(2): 222-234 https://doi.org/10.54367/fiat.v2i2.1770.

