TABELLIUS Journal of Law
ISSN 2988-6201
published by
Master of Notarial Law
Faculty of Law
Universitas Islam Sultan Agung
Semarang

Legal Construction of Dual Authentication for Notary Digital Account Protection

Muhammad Anugrah Ubaidillah Yakob Udi
Faculty of Law, Universitas Islam Sultan Agung, Semarang, Indonesia. Email: Muhammadanugrahubaidillah@gmail.com

Abstract. *The digitalization of legal administration has made notary digital accounts a professional identity in electronic systems, but reliance on a single password poses risks of unauthorized access, data leakage, and misattribution of responsibility. This study aims to analyze the legal construction of dual authentication to strengthen the protection of notary digital accounts. The study uses normative legal methods with a statutory and conceptual approach; legal materials are collected through literature studies and analyzed prescriptively. The results show that the dual authentication obligation has not been specifically regulated for all notary digital accounts, but its normative basis can be constructed from the notary's obligation to act trustworthy and diligently, maintain the confidentiality of his position, the administrator's obligation to provide a reliable and secure system, and provisions for the protection of personal data. The required legal construction places dual authentication as a mandatory minimum risk-based standard, accompanied by re-verification for actions with legal consequences, device and access rights restrictions, audit trails, suspicious access notifications, account recovery, and the division of responsibility based on the area of control and contribution of errors.*

Keywords: *Account; Authentication; Construction; Legal; Protection.*

1. Introduction

Digital transformation has shifted some notary administration functions to electronic systems. Notary accounts are used to access legal administration services, upload documents, submit data, and submit requests that can have administrative and legal consequences. This change increases efficiency but also expands the scope of official confidentiality, extending beyond the contents of deeds to include credentials, devices, activity records, and party data. Research on

data protection in cyber notaries confirms that digitalization must be accompanied by mechanisms to prevent unauthorized access.[1]

A notary's digital account differs from a personal account because access rights stem from official authority. When credentials are acquired by another party, the system can still record data changes or service requests as if they were made by the notary. This misuse not only harms the account holder but also undermines the integrity of legal administration and trust in digital services. Other cases of notary account use demonstrate that this issue has entered the ethical, administrative, and legal realms.[2]

The notarial law requires notaries to act with integrity, honesty, and thoroughness, and to maintain the confidentiality of all information obtained in the course of their duties. However, this norm does not specify the control of authentication factors, employee access restrictions, account recovery, and division of responsibility in the event of misuse. Meanwhile, the electronic systems law requires a reliable and secure system, but has not yet established sectoral standards that explicitly bind all notary digital accounts.[3]

This gap is crucial because single-password authentication is no longer sufficient for high-value accounts. Passwords can be obtained through phishing, data breaches, social engineering, credential reuse, or internal negligence. A weak security culture also encourages the practice of sharing accounts among employees without auditable controls.[4]Security research shows that additional authentication challenges can decrease the success of account takeovers.[5]

Authentication defines the link between digital identity, electronic actions, proof, and accountability. Systems that only verify passwords cannot always distinguish the account owner from the party who obtained the credentials. As a result, notaries can be held liable for actions they did not perform, while injured parties

[1]Octarina, Nynda Fatmawati., Fernanda, Fadila., Dewi, Fironika Tri Asni., & Adjie, Habib. (2024). "The Urgency of Regulation of Data Protection for the Parties in Cyber Notary". in Jurnal Akta, Volume 11 Number 3, pp. 630–650. https://doi.org/10.30659/akta.v11i3.39748.
[2]Nagaring, Alyah Nanda Rayan., & Arief, Supriyadi A. (2026). "Enforcement of Administrative Sanctions against Notaries Who Illegally Misuse Other Notary Accounts." in Notary Law Journal, Volume 5 Number 1, pp. 35–45. https://doi.org/10.32801/nolaj.v5i1.135.
[3]Ridwan, Masrur. (2020). "Reconstruction of Notary Position Authority and Implementation of Basic Concepts of Cyber Notary." in Jurnal Akta, Volume 7 Number 1, pp. 61–68. https://doi.org/10.30659/akta.v7i1.9432.
[4]Alshaikh, M. (2020). "Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective". in Computers & Security, Volume 98, Article 102003. https://doi.org/10.1016/j.cose.2020.102003.
[5]Doerfler, Periwinkle., Thomas, Kurt., Marincenko, Maija., Ranieri, Juri., Jiang, Yu., Moscicki, Adam., & McCoy, Damon. (2019). "Evaluating Login Challenges as a Defense Against Account Takeover". in Proceedings of the World Wide Web Conference, p. 372–382. https://doi.org/10.1145/3308558.3313481.

struggle to prove the true perpetrator. The reliability of digital identity is also a crucial element in building trust in electronic government services.[6]

Previous research has focused more on electronic deeds, the authority of cyber notaries, data protection of the parties, and the evidentiary power of digital products.[7]The study did not specifically address the security of notary digital accounts as an object of legal protection. The novelty of this research lies in the construction of dual authentication as a minimum standard for official security, linking prudence, confidentiality, legal certainty, personal data protection, auditability, and division of responsibility.

Based on this description, this study aims to analyze the legal construction of dual authentication to strengthen the protection of notary digital accounts.

2. Research Methods

This research is a normative legal study with a statutory and conceptual approach. The research specifications are prescriptive. Primary legal materials include regulations regarding notary positions, electronic systems, personal data protection, and public electronic systems. Secondary legal materials consist of books, journal articles, research findings, and digital identity security guidelines. Legal materials were collected through literature review and analyzed by assessing their relevance, consistency, gaps, and the need for normative reform.[8]

3. Results and Discussion

3.1. Legal Status of Notary Digital Accounts

A notary's digital account is an electronic identity that connects the office holder to the legal administration system. Its status cannot be equated with a commercial account, as access rights arise from state-granted authority. Through this account, notaries enter data, upload documents, submit applications, receive notifications, and obtain system output. Account ownership thus represents control over the means of exercising official authority.

---

[6]Addo, Atta., & Senyo, PK (2021). "Advancing E-Governance for Development: Digital Identification and Its Link to Socioeconomic Inclusion". in Government Information Quarterly, Volume 38 Number 2, Article 101568. https://doi.org/10.1016/j.giq.2021.101568; Janssen, Marijn et al. (2018). "Trustworthiness of Digital Government Services: Deriving a Comprehensive Theory through Interpretive Structural Modeling". in Public Management Review, Volume 20 Number 5, p. 647–671. https://doi.org/10.1080/14719037.2017.1305689.

[7]Kuspratomo, Yudha Priyo., Hasanah, Lailatul Nur., & Wahyuningsih, Sri Endah. (2019). “Making Implementation Deed Electronically Based on Law of Notary”. in Jurnal Akta, Volume 6 Nomor 4, pp. 691–696. https://doi.org/10.30659/akta.v6i4.7666; Lestari, Sulistyani Eka et al. (2024). “Navigating Legal Transformation: Challenges and Prospects of Cybernotary in Enhancing Public Service Efficiency in Indonesia”. in Jurnal Akta, Volume 11 Nomor 4, pp. 1222–1245. https://doi.org/10.30659/akta.v11i4.40781.

[8]Marzuki, Peter Mahmud. (2017). Legal Research. Jakarta: Kencana, pp. 35–47.

Consequently, every digital action must be accurately attributed to an authorized user. Identification, authentication, and authorization are distinct stages: identification reveals who claims to be the user, authentication proves the identity claim, and authorization determines which actions can be performed. A failure to authenticate undermines the entire process because system records only show the account being used, not the person actually operating it.

The legal value of accounts increases because system output can form the basis for further administrative processes. When an account is used by another party, the electronic record still formally identifies the notary as the perpetrator. Legal certainty requires a mechanism that links account identity to human identity, especially in actions affecting legal entity data, the status of parties, or documents that have evidentiary significance.

Accounts also serve as access points to personal data and confidential information. The obligation to maintain confidentiality of the contents of deeds and the parties' statements includes safeguarding passwords, verification codes, authentication devices, electronic documents, registered email addresses, and employee access. The implementation of cyber notary services must be integrated with data protection to ensure that technology does not diminish the essence of official confidentiality.[9]

Delegating administrative work is not synonymous with transferring job identity. Employees can assist in data preparation through individual accounts with limited privileges, but final approval must remain under the control of a notary. Therefore, digital credentials should be treated on a par with stamps, signatures, minutes, and protocols: they should not be freely handed over to others and must be supported by a verifiable trail of activity.

Legal certainty for digital accounts requires at least three layers. First, identity certainty, namely the system's ability to verify the identity of the actual user. Second, action certainty, namely recording the time, device, type of service, and data processed. Third, responsibility certainty, namely the ability to distinguish between notary actions, internal negligence, administrator weaknesses, and third-party attacks. Without these three layers, electronic records only prove that an account was used, but do not prove the actual perpetrator.

3.2. Normative Construction of Dual Authentication

Account security obligations can be derived from the principles of trustworthiness, due diligence, and official confidentiality. Trustworthiness relates to the trust of the state and the public, while due diligence requires actions commensurate with

[9]Octarina, Nynda Fatmawati et al. (2024). "The Urgency of Regulation of Data Protection for the Parties in Cyber Notary." in Jurnal Akta, Volume 11 Number 3, pp. 638–644. https://doi.org/10.30659/akta.v11i3.39748.

the level of risk. In the digital context, these principles require access restrictions, mastery of authentication factors, activity verification, and incident reporting.

The Electronic Information and Transactions Law recognizes electronic information and documents and requires providers to provide reliable, secure, and accountable systems. Reliability means not only that the system is operational, but also that it is able to prevent unauthorized access, maintain data integrity, and link actions to authorized users.[10]Government Regulation Number 71 of 2019 strengthens this through the obligation to maintain authenticity, integrity, availability, confidentiality, and provide an audit trail. The explanation of Article 40 paragraph (1) letter a mentions a combination of at least two authentication factors in testing the authenticity of identity and authorization.

These two-factor provisions constitute the most explicit normative basis, but they exist within the context of electronic agent regulations and therefore have not yet become a sector-wide obligation for all notary accounts. The gap that arises is not a lack of principles, but rather a lack of operational standards that define the type of authenticator, actions requiring re-verification, recovery procedures, incident reporting, and consequences for non-compliance.

The Personal Data Protection Law adds an obligation to implement adequate technical and organizational measures. Notary accounts can open access to identity, address, family information, corporate data, and supporting documents. Account compromise can lead to unauthorized access, modification, or disclosure of data. Dual authentication is therefore a preventative measure to meet the principle of secure personal data processing.[11]

System administrators control application architecture, logging, session control, account recovery, and authentication design; while notaries control credentials, devices, and user behavior within their offices. Security standards should divide responsibilities based on their respective areas of control. Assigning the notary full responsibility ignores system design weaknesses, while exempting the notary from the obligation to maintain professional identity.

Based on the synthesis of norms, securing a notary's digital account must be built on four layers. First, the obligation of office places credential security as part of trustworthiness, accuracy, and confidentiality. Second, electronic systems law requires administrators to provide a reliable, secure, and accountable system. Third, provisions on authenticity, authorization, and audit trails provide the basis for implementing two-factor authentication. Fourth, personal data protection law requires technical and organizational measures to prevent unauthorized access.

[10]Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, specifically Articles 5 and 15; Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.
[11]Law Number 27 of 2022 concerning Personal Data Protection, specifically Article 35, Article 39, and Article 46.

These four layers are complementary and cannot be solely the responsibility of one party.

The regulatory direction is to position dual authentication as both a job obligation and a system design obligation. Notaries are required to safeguard credentials and the second factor, while administrators are required to provide authentication tools, segregated access rights, comprehensive logs, recovery procedures, and incident response. This construction bridges the gap between general norms and operational needs without having to wait for legislative changes, as long as the technical obligations are formulated through regulations that align with the authority of the regulator.Normatively, dual authentication should not be understood simply as a login feature. This mechanism must legally bind notaries, restrict employee use of credentials, and generate verifiable electronic evidence. Thus, dual authentication simultaneously strengthens preventative protection and provides repressive evidence in the event of abuse.

3.3. Dual Authentication in Notary Law and Doctrine

Dual authentication uses two distinct categories of identity proof, such as something the user knows and something they possess. If the password is discovered by another party, access remains blocked because the second factor remains with the legitimate owner. For notary accounts, the second factor should not be placed on office phones or employee devices, as this practice simply changes the way credentials are shared.[12] From a legal protection perspective, dual authentication is a preventative measure. Prevention is more relevant than recovery alone, as a single unauthorized access can result in data changes, service requests, or document leaks in a short time. Repressive protection is still necessary through account blocking, log review, data recovery, and sanction enforcement, but its effectiveness depends on the quality of activity records.

The principle of legal certainty requires objective minimum standards. The general recommendation to "safeguard accounts" fails to specify the technology, procedures, or limits of liability. Standards should include prohibitions on credential sharing, mandatory second-factor authentication, rigorous verification when changing devices, incident reporting, and audit trail retention. This clarity protects the public while preventing subjective assessments of negligence. Dual authentication also strengthens the doctrine of official liability. Responsibility cannot be attributed simply because an account was used. The assessment must consider whether the notary shared credentials, ignored warnings, lost the device without reporting it, or otherwise met standards but fell victim to system

[12]Ometov, Aleksandr et al. (2018). “Multi-Factor Authentication: A Survey”. in Cryptography, Volume 2 Number 1, Article 1. https://doi.org/10.3390/cryptography2010001; Otta, Subhendu Prakash et al. (2023). “A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure”. in Future Internet, Volume 15 Number 4, Article 146. https://doi.org/10.3390/fi15040146; Temoshok, David et al. (2025). Digital Identity Guidelines: Authentication and Authenticator Management. NIST Special Publication 800-63B-4, Parts 2–4.

weaknesses. A contribution-to-fault approach results in a fairer allocation of responsibility.

The doctrine of official responsibility also requires personal control over actions that give rise to legal consequences. Employee assistance is only permissible during the preparatory phase and must be limited through shared access rights. Notary offices should have written procedures for creating and changing passwords, using devices, revoking employee access, data backup, and incident reporting. These internal procedures are crucial because the effectiveness of dual authentication remains dependent on user behavior and office governance. Studies on the certainty of proof in cyber notary show that regulatory ambiguity can reduce trust in digital products.[13]While the focus wasn't on electronic deed creation, the findings are relevant because the reliability of digital products begins with the reliability of user identity. A complete document remains problematic if the system cannot verify who submitted or approved it.

3.4. Legal Construction Model and Division of Responsibility

An ideal regulatory model should require at least two independent authentication factors. The first factor can be a password or PIN, while the second factor can be an authenticator app, passkey, security key, device certificate, or device-bound biometric. Text messaging can be used as a transition mechanism, but it shouldn't be the sole option due to the risks of number takeover and social engineering. The second factor must be within the notary's personal control. If employees require access, the organizer must provide individual accounts with limited privileges. Final approval still requires notary authentication. The system should also implement re-verification for application submissions, changes to critical data, device registration, email or phone number changes, and account recovery.

Device restrictions, session management, and anomaly detection should complement authentication. Notaries should be able to view and remove connected devices and receive notifications when new logins occur. Inactive sessions should expire automatically, while unusual patterns, such as multiple requests in a short period of time or access from a new location, should trigger additional checks. The audit trail should, at a minimum, include the time, user identity, type of action, data changed, device, network address, authentication method, and verification result. The log should be protected from tampering and available through authorized audit procedures. Account recovery mechanisms should also be equivalent to or stronger than normal authentication, including notification to legacy channels, revocation of lost authenticators, and a waiting period for high-risk actions.[14] Incident management should establish a notary's

[13]Iswari, Katrin Yogi et al. (2024). "Legal Certainty of the Proof Power of Notary Deeds in the Concept of Cyber Notary according to Indonesian Positive Law". in Deed Journal, Volume 11 Number 3, p. 662–684. https://doi.org/10.30659/akta.v11i3.39750.
[14]Iorga, Michaela et al. (2020). NIST Cloud Computing Forensic Science Challenges. NISTIR 8006, p. 11–18. https://doi.org/10.6028/NIST.IR.8006.

obligation to immediately report lost devices, unrecognized code requests, or suspicious transactions. Organizers are required to provide emergency channels, block access, secure logs, assess the impact, and fulfill notification obligations if the incident involves personal data. Delays by each party can be the basis for assessing liability.

The division of responsibilities must adhere to the principle of control. Notaries are responsible for passwords, authenticators, devices, and employee behavior in their offices. Organizers are responsible for authentication design, application security, logs, anomaly detection, recovery, and incident response. The Notary Supervisory Board assesses job compliance, while professional organizations provide education and operational guidelines. Implementation of the regulations should be gradual. The initial phase includes activating dual authentication, updating contact data, and registering devices. Subsequent phases include individual employee accounts, re-verifying transactions, and accessing activity history. Subsequent phases include anomaly detection, regular audits, and integrating complaint and audit mechanisms. A gradual approach minimizes service disruption, but each phase must have deadlines and compliance indicators to ensure that obligations do not cease to be administrative recommendations.

Sanctions need to be differentiated between technical errors, serious negligence, and malicious acts. Late updates can result in warnings and corrections; deliberate sharing of credentials can be subject to ethical and administrative sanctions; and unauthorized access and data manipulation should be prosecuted under criminal and civil law. A two-tiered arrangement is more appropriate: ministerial regulations outline the core obligations, while technical standards address authenticator types, session parameters, recovery, log retention, and anomaly indicators. This structure maintains legal certainty while enabling technological adaptation.[15]

4. Conclusion

The legal framework for dual authentication for digital notary accounts can be built on the notary's obligation to act trustworthy and diligently, maintain the confidentiality of their position, the administrator's obligation to provide a reliable and secure electronic system, and the obligation to protect personal data. The current legal weakness lies in the absence of sectoral norms that explicitly require dual authentication for all digital notary accounts and regulate their use procedures. A notary's digital account represents their official identity because it is used to access data, request services, and perform actions that can have legal consequences. Therefore, dual authentication must be constructed as both preventative legal protection and electronic evidence infrastructure. This

[15]Lestari, Sulistyani Eka et al. (2024). “Navigating Legal Transformation: Challenges and Prospects of Cybernotary in Enhancing Public Service Efficiency in Indonesia.” in Jurnal Akta, Volume 11 Number 4, pp. 1222–1245. https://doi.org/10.30659/akta.v11i4.40781.

framework includes re-verification for high-risk actions, personal control of the second factor, device and session restrictions, separation of employee access rights, a complete audit trail, anomaly notification, and secure account recovery. Liability must be determined based on the scope of control and the contribution of errors so that notary actions, internal negligence, system weaknesses, and third-party attacks can be proportionally distinguished. Governments and legal administration service providers should establish dual authentication as a mandatory minimum standard through technical regulations governing authenticator types, device registration, transaction verification, account recovery, log retention, incident reporting, and non-compliance sanctions. Systems should provide individual accounts for employees with limited privileges, while final approval remains through notary authentication. Notaries should discontinue the practice of sharing usernames, passwords, and verification codes and establish internal procedures regarding work devices, revoking employee access, data backup, and reporting suspicious events. The Notary Supervisory Board and professional organizations should incorporate digital security compliance into training, continuing education, and job examinations. The implementation of these standards needs to be periodically evaluated through audits and incident simulations to ensure that dual authentication does not remain a formality but actually increases legal certainty, data protection for parties, and trust in digital notarial administration.

5. References

Journals:

Addo, Atta., & Senyo, P. K. (2021). "Advancing E-Governance for Development: Digital Identification and Its Link to Socioeconomic Inclusion". *Government Information Quarterly*, 38(2), 101568. https://doi.org/10.1016/j.giq.2021.101568.

Alshaikh, M. (2020). "Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective". *Computers & Security*, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003.

Doerfler, Periwinkle., Thomas, Kurt., Marincenko, Maija., Ranieri, Juri., Jiang, Yu., Moscicki, Adam., & McCoy, Damon. (2019). "Evaluating Login Challenges as a Defense Against Account Takeover". *Proceedings of the World Wide Web Conference*, 372–382. https://doi.org/10.1145/3308558.3313481.

Iorga, Michaela., Feldman, Larry., Barton, Robert., Martin, Michael J., Goren, Nedim S., & Mahmoudi, Charif. (2020). *NIST Cloud Computing Forensic Science Challenges*. NISTIR 8006. https://doi.org/10.6028/NIST.IR.8006.

Iswari, Katrin Yogi., Adzania, Pelangi., Novilawati, Rizka., & Samosir, Tetti. (2024). "Legal Certainty of the Proof Power of Notary Deeds in the Concept of Cyber Notary according to Indonesian Positive Law". *Jurnal Akta*, 11(3), 662–684. https://doi.org/10.30659/akta.v11i3.39750.

Janssen, Marijn., Rana, Nripendra P., Slade, Emma L., & Dwivedi, Yogesh K. (2018). "Trustworthiness of Digital Government Services: Deriving a

Comprehensive Theory through Interpretive Structural Modelling". *Public Management Review*, 20(5), 647–671. https://doi.org/10.1080/14719037.2017.1305689.

Kuspratomo, Yudha Priyo., Hasanah, Lailatul Nur., & Wahyuningsih, Sri Endah. (2019). "Making Implementation Deed Electronically Based on Law of Notary". *Jurnal Akta*, 6(4), 691–696. https://doi.org/10.30659/akta.v6i4.7666.

Lestari, Sulistyani Eka., Thoif, Mokh., Widodo, Teguh Endi., & Minan. (2024). "Navigating Legal Transformation: Challenges and Prospects of Cybernotary in Enhancing Public Service Efficiency in Indonesia". *Jurnal Akta*, 11(4), 1222–1245. https://doi.org/10.30659/akta.v11i4.40781.

Nagaring, Alyah Nanda Rayan., & Arief, Supriyadi A. (2026). "Penegakan Sanksi Administratif terhadap Notaris yang Melakukan Penyalahgunaan Akun Notaris Lain secara Ilegal". *Notary Law Journal*, 5(1), 35–45. https://doi.org/10.32801/nolaj.v5i1.135.

Ometov, Aleksandr., Bezzateev, Sergey., Mäkitalo, Niko., Andreev, Sergey., Mikkonen, Tommi., & Koucheryavy, Yevgeni. (2018). "Multi-Factor Authentication: A Survey". *Cryptography*, 2(1), 1. https://doi.org/10.3390/cryptography2010001.

Otta, Subhendu Prakash., Panda, Sujata Kumari., & Gupta, M. (2023). "A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure". *Future Internet*, 15(4), 146. https://doi.org/10.3390/fi15040146.

Octarina, Nynda Fatmawati., Fernanda, Fadila., Dewi, Fironika Tri Asni., & Adjie, Habib. (2024). "The Urgency of Regulation of Data Protection for the Parties in Cyber Notary". *Jurnal Akta*, 11(3), 630–650. https://doi.org/10.30659/akta.v11i3.39748.

Ridwan, Masrur. (2020). "Reconstruction of Notary Position Authority and Implementation of Basic Concepts of Cyber Notary". *Jurnal Akta*, 7(1), 61–68. https://doi.org/10.30659/akta.v7i1.9432.

Temoshok, David., Choong, Yee-Yin., Regenscheid, Andrew., & Fenton, James. (2025). *Digital Identity Guidelines: Authentication and Authenticator Management*. NIST Special Publication 800-63B-4.

Books:

Marzuki, Peter Mahmud. (2017). *Penelitian Hukum*. Jakarta: Kencana.

Regulation:

Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Law Number 27 of 2022 concerning Personal Data Protection.

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.