International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 21-04-2024, Accepted: 12-05-2024, Published: 06-06-2024
Volume 10, Issue 3, 2024, Page No. 170-174

Authority of implementing electronic know your customer (E-KYC) based on national identity number towards clients in creating authentic deeds in Indonesia

Asih Susilowati[1], Neni Sri Imaniyati[2], Taufik Kurohman[3]
[1] Faculty of Law, Universitas Islam Bandung, Bandung, Indonesia
[2] Lecturers, Faculty of Law, Universitas Islam Bandung, Bandung, Indonesia
[3] Lecturer, Universitas Pamulang, Tangerang Selatan, Indonesia

Abstract
In the context of implementing the electronic identity verification process known as electronic Know Your Customer (e-KYC) based on the National Identity Number (NIK) by notaries when creating authentic deeds, there are deficiencies in the regulations governing this matter. A normative legal research approach, utilizing secondary data such as government regulations and laws, proves to be useful in identifying ambiguities in the existing rules. The Information and Electronic Transactions Act No. 19 of 2016 (UU ITE) serves as relevant legal grounds; however, the application of e-KYC by notaries requires more specific implementing regulations, particularly concerning the role of notaries as electronic certification authorities, commonly known as "Cyber Notaries." In developing these implementing regulations, several crucial aspects must be considered. Firstly, the authority of notaries as Cyber Notaries needs to be clearly defined. Secondly, the procedures and standards for identity verification through e-KYC must be detailed. Thirdly, strict protection of personal data must be ensured in accordance with regulations on data privacy protection. Fourthly, these regulations should also be closely related to other regulations, such as the Population Administration Law and rules pertaining to the position of notaries. Finally, mechanisms for law enforcement in cases of violations or misuse of the e-KYC process by notaries must also be clearly defined. With comprehensive and detailed implementing regulations in place, notaries can carry out the e-KYC process with greater confidence and effectiveness, thus ensuring the sustainability of electronic authentic deed creation while maintaining the security and trust of all involved parties.

Keywords: Notary authority, electronic know your customer, electronic certification

Introduction

The development of information technology has significantly transformed the landscape of interaction between individuals and information service providers in society. Various fields, ranging from trade, governance, finance, transportation, industry, to tourism, have adopted online-based technologies to provide services to the public. The workflow of these systems involves several key stages, including data collection, data storage, data processing, information production, and delivery of information to end users.

The implementation of electronic Know Your Customer (e-KYC) brings several significant benefits in the customer identity verification process and compliance obligations for financial institutions. One of the main advantages is faster and more flexible service access. With e-KYC, identity verification can be done electronically and in a shorter time compared to traditional methods that require face-to-face meetings. This allows customers to access financial services more quickly and easily. The use of technology in this process can reduce the time required for customer identity verification, thereby improving the operational efficiency of financial institutions.

Additionally, e-KYC can also reduce administrative costs associated with manual identity verification processes. This includes costs for document processing, travel expenses for face-to-face meetings, and other administrative fees. By eliminating the need for face-to-face meetings, e-KYC reduces costs and time required by both customers and financial institutions. These cost savings can benefit both financial institutions and customers. Financial institutions can allocate their resources more efficiently, while customers can enjoy a faster and more convenient process in accessing financial services [1].

The fact that information technology has become a basic necessity in daily life has brought significant consequences, especially concerning the protection of personal data. The increase in digital services and the widespread use of personal data have underscored the importance of protecting personal data in the digital environment. In Indonesia, although there is the Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), there is no specific regulation that comprehensively governs the protection of personal data. However, in 2016, the Indonesian government enacted the Government Regulation in Lieu of Law (Perppu) Number 82 of 2012 concerning Electronic Information and Transactions (ITE), which later became the ITE Law, providing a legal basis for the protection of personal data.

Regarding personal electronic data, Notaries in creating electronic deeds are also regulated in Article 15 paragraph (3) of the 2014 Notary Law which refers to "other authorities regulated in the legislation," including the authority to certify transactions conducted electronically, create deeds of waqf pledges, and aircraft mortgages. However, the issue of ambiguity regarding the authority of notaries to certify (Amiruddin, 2018) electronically conducted transactions is an important issue in the current legal and technological context. Although the Notary Law provides a legal basis for such authority, confusion or ambiguity in the interpretation or application of these rules may still occur.

A Cyber Notary, also known as an electronic notary, is an entity or individual authorized to perform notarization or similar processes electronically. They are responsible for validating and ensuring the authenticity of electronic documents, digital signatures, or other transactions. Cyber notaries play a crucial role in ensuring the integrity and validity of electronic transactions, similar to the role of traditional notaries in physical documents. By understanding these concepts, we can better comprehend how the process of certifying electronic transactions works and the role of cyber notaries in safeguarding the security and validity of such transactions.

Article 15 paragraph (3) of the Notary Law revision itself uses the term certification. In terminology, certification means "the act of certifying, signifying a process, method, or making something certifiable." [2] The result of such certification is a certificate that serves as "a written or printed statement or document from an authorized person that can be used as proof of ownership or an event." [3] The definition of certification according to Emma Nurita is "a procedure where a third party provides written assurance that a product, process, or service has met specific standards, based on an audit conducted with agreed-upon procedures."

The explanation you provided indicates that notaries have the authority to certify transactions conducted through cyber notaries. The term "certification" originates from the English word "certification," which means a statement or verification [4]. The definition of certification is a procedure in which a third party provides written assurance that a product, process, or service has met specific standards, based on an audit conducted with agreed-upon procedures [5].

The implementation of e-KYC (Know Your Customer electronically) in the process of creating authentic deeds by Notaries has many benefits, especially in preventing identity theft and related criminal activities. Here are some of the key benefits of using e-KYC in the notary practice:

1. Prevention of Identity Fraud: e-KYC helps in verifying the identity of clients electronically, reducing the risk of identity theft and fraudulent activities during the creation of authentic deeds.
2. Enhanced Security: By using electronic verification methods, the security of the identity verification process is improved, making it more difficult for unauthorized individuals to impersonate clients.
3. Compliance with Regulations: Implementing e-KYC helps notaries comply with regulatory requirements related to customer identification and verification, reducing the risk of legal issues related to identity fraud.
4. Efficiency: The use of e-KYC streamlines the identification and verification process, saving time and resources for both notaries and clients.
5. Reduced Risk of Criminal Activities: By accurately verifying the identities of clients, e-KYC reduces the risk of notaries inadvertently participating or aiding in fraudulent activities, such as being witnesses to false testimonies in court.

Overall, the adoption of e-KYC in notarial practices brings significant advantages in terms of security, compliance, efficiency, and risk mitigation related to identity fraud and criminal activities.

This highlights the urgent need for Notaries to utilize e-KYC tools to prevent criminal activities in creating authentic deeds. Analyzing the legal certainty of implementing the electronic Know Your Customer (e-KYC) system based on the National Identity Number (NIK) for Notaries in creating authentic deeds, along with the comparison of legal implications applicable in Singapore, is crucial.

An analysis regarding the legal certainty of implementing the electronic Know Your Customer (e-KYC) system based on the National Identity Number (NIK) for Notaries in creating authentic deeds is essential, especially in the context of preventing criminal activities and enhancing transaction security. I can provide general information on this matter, but for a comparison of the legal implications applicable in Singapore, it would be best to consult with a legal expert familiar with Singaporean law specifically.

Generally, the use of e-KYC in the practice of Notaries in Indonesia brings about several relevant legal implications: (a) Identity Certainty: e-KYC based on NIK can help ensure the authenticity of the identities of parties involved in creating authentic deeds. This reduces the risk of identity forgery and related criminal activities. (b) Legal Compliance: Implementing e-KYC helps Notaries comply with regulations concerning customer identification and verification. This can reduce the risk of legal issues related to false identities or illegal transactions. (c) Efficiency Enhancement: Electronic identification processes can improve efficiency in creating authentic deeds, reducing the time and costs required for identity verification processes. (d) Personal Data Protection: In the context of e-KYC, protecting personal data becomes crucial. Notaries must ensure the security and confidentiality of customer data accessed and stored in the e-KYC system.

A comparison with Singaporean law may reveal differences in regulations, implementation, and legal handling related to e-KYC. Therefore, it's advisable to seek a more specific perspective from a legal expert familiar with the legal context in Singapore.

Research Method

The research method used is normative legal research, which relies on secondary data as the basis. These secondary data include literature such as Government Regulation Number 40 of 2019 on Population Administration, the Law on Personal Data Protection, Law Number 19 of 2016 on Information and Electronic Transactions, as well as Law Number 24 of 2013 on Population Administration and Law Number 2 of 2014 on amendments to Law Number 30 of 2004 on Notary Positions. The literature encompasses primary legal materials that are binding, secondary legal materials that provide explanations, and tertiary legal materials such as the Indonesian Dictionary. Data obtained from this literature is then processed and analyzed qualitatively to understand the phenomenon under study, namely the protection of personal data in electronic transactions. This analysis is important for understanding the impact and implications of existing regulations on the protection of personal data in the context of information technology [6].

Result and Discussion

The concept of protecting personal data privacy based on National Identity Numbers.

The concept of protecting personal data that you've outlined here emphasizes individuals' rights to control their personal information. This includes the right to decide whether to share their personal data and, if so, with whom and under what circumstances that data will be shared. Additionally, individuals have the right to determine the terms or conditions that must be met by the party receiving their data within the community or society context [7]. The importance of this concept lies in the recognition that one's personal information is a part of their human rights and must be safeguarded from misuse, unauthorized disclosure, or unethical use. In the context of an increasingly interconnected and digitized world, the need to protect personal data has become increasingly urgent.

Personal data is a part of every individual's privacy, which is reflected in the second principle of Pancasila that states "A Just and Civilized Humanity." The definition of personal data according to the Population Administration Law is "Specific individual data that is stored, maintained, and protected for its accuracy and confidentiality." (Law, 2013) Protecting personal data is necessary so that users can confidently provide their data to the system for processing and ease of life.

According to the Population Administration Law, personal data that must be protected includes: "Family Card Number; National Identity Number (NIK); date/month/year of birth; information about physical and/or mental disabilities; mother's NIK; father's NIK; and certain important event records." According to the Personal Data Protection Law, the definition of personal data includes data about an individual, whether alone or in combination, through electronic or non-electronic systems. Meanwhile, under the Criminal Code, personal data refers to objects that can be subject to property rights, which means theft of personal data can be penalized and/or held accountable [8].

Indonesia has taken steps to regulate the protection of personal data, although it does not yet have a specific law governing this matter. However, there are several laws and regulations related to the protection of personal data in Indonesia, including:

1. **Banking Law Number 10 of 1998 (hereinafter referred to as the Banking Law):** Article 1 paragraph (28) states that "Bank secrecy is everything related to customer deposits and their deposits." This explains that any information related to customer deposits and their deposits in banks is sensitive and confidential. Also, Article 40 paragraph (1) states that "Banks are obliged to maintain the confidentiality of information about customer deposits and their deposits, except as referred to in Article 41, Article 41A, Article 42, Article 44, and Article 44A." Therefore, banks have an obligation to protect all information or data regarding customer deposits and their deposits.

2. **Telecommunications Law Number 36 of 1999 (hereinafter referred to as the Telecommunications Law):** Article 42 paragraph (1) of the Telecommunications Law states that "Telecommunications service providers must maintain the confidentiality of information transmitted and/or received by telecommunications service customers through telecommunications networks and/or services provided." Although this article does not explicitly mention the protection of personal data, it can be interpreted as covering the protection of personal information of customers transmitted or received through telecommunication services.

3. **Electronic Information and Transactions Law Number 19 of 2016 (hereinafter referred to as the ITE Law):** Article 26 paragraph (1) is the only article that explicitly emphasizes the protection of personal data must be carried out. The ITE Law also regulates prohibited acts related to the field of electronic information, although not specifically focused on personal data, in Articles 27 to 37. These articles broadly prohibit unauthorized and intentional misuse of electronic information that could harm others, especially the information owner.

The Concept of Implementing Cyber Notary in Singapore

Singapore is often regarded as an advanced country in the world and is well-known for its high achievements in various global measurements due to several factors, including efficient government policies, good infrastructure, quality education, and a conducive business climate. As a result, it performs well in the Human Development Index, Global Competitiveness Index, and Ease of Doing Business Index. There is ample empirical research that proves Singapore's progress [9]. The public administration and bureaucracy in Singapore are heavily influenced by the 140 years of British colonial rule (1819-1959), which continued after Singapore emerged as an autonomous entity within Malaysia in 1963 and separated from Malaysia in 1965. The distinctive British Commonwealth pattern ultimately significantly influenced the formation of its political, economic, and particularly public administration and bureaucracy foundations. Moreover, [10] in line with the overall parliamentary government model, the Parliament in Singapore utilizes various standing committees to carry out its tasks, such as the Selection Committee, Public Accounts Committee, Estimates Committee, and others [11].

In a contemporary context, public administration and bureaucracy in Singapore have adopted a framework known as "Dynamic Governance," which consists of three main concepts [12]: forward thinking, rethinking, and thinking across boundaries. Through the concept of thinking ahead, the government is encouraged to anticipate future scenarios through conceptualization processes. Regulations must be created to protect the people from threats and challenges arising from new situations. The concept of thinking again emphasizes the government's ability to reassess and adapt to changing circumstances.

Here are the detailed explanations for each concept regarding understanding and developing regulations that are responsive to societal needs and changes:

1. **Responsive Regulation:** Adapting regulations to changing societal needs and long-term conditions requires continuous adjustments. It's crucial to ensure that existing policies and regulations remain relevant and effective. In this context, the government needs mechanisms that allow them to monitor changes, receive feedback from the public, and make necessary adjustments to regulations.

2. **Thinking Across:** This concept refers to the government's ability to think across sectors and disciplines. This enables them to gain a more comprehensive understanding of the issues at hand and seek innovative and effective solutions. Thinking across also allows the government to identify opportunities for cross-sector collaboration that can enhance policy efficiency and effectiveness.

3. **Able People:** This emphasizes the importance of having qualified and trained personnel within the government. These individuals should possess good analytical skills, deep understanding of various issues, as well as strong communication and collaboration skills. They are key to implementing cross-thinking concepts and generating adaptive policies.

4. **Agile Process:** Flexible and responsive processes are crucial in producing adaptive policies. The government needs a system that allows them to quickly respond to changing conditions or new inputs. This enables them to make necessary adjustments to regulations without getting stuck in rigid bureaucracy.

5. **Adaptive Policies and Dynamic Governance Outcomes:** The outcomes of applying the above concepts are adaptive policies and dynamic governance results. This means policies and governance that can adapt to environmental changes and societal needs, resulting in more effective and sustainable outcomes. By applying these concepts, the government can be more effective in responding to challenges and opportunities faced by society and the ever-changing environment. This helps create a more dynamic and responsive regulatory system, which in turn can enhance the well-being and progress for all involved parties.

The Singapore government launched "Singapore One," the first nationwide broadband infrastructure. It covers 99% of Singapore's territory, distributing broadband technology capabilities to schools, businesses, homes, libraries, and community centers. Additionally, in 1999, E-Citizen One Stop was launched, similar to the One-Stop Integrated Service (PTSP) in Indonesia, as a unified interface for public services for the community [13].

The enhancement of information technology infrastructure in Singapore has strengthened e-government services and internet connectivity in the country. Singapore has become a model for e-government implementation, with every government institution having an electronic portal to provide services to citizens. This has improved public administration efficiency and government service accessibility for the public. The authority responsible for e-government in Singapore is the Infocom Development Authority (IDA), and the main e-government portal in Singapore is E-Citizen.

In the context of Electronic Notary or "e-Notary" in Singapore, the relevant law is the Singapore Electronic Transactions Act 2010 (ETA 2010). For Electronic Notaries, this law provides the legal basis for using electronic records as valid evidence in electronic notarization processes. This indicates that Singapore has adopted a relevant legal framework to support the use of technology in legal processes, including notarization and electronic transactions.

Authority for Implementing Electronic Know Your Customer (e-KYC) Based on National Identity Number in Notarial Deed Making in Indonesia

According to Article 1 number 7 of Law Number 2 Year 2014 concerning Notary Position, it states that: "Notarial Deed, hereinafter referred to as Deed, is an authentic deed made by or in the presence of a Notary according to the form and procedures stipulated in this Law."

A Notary is a public official appointed by the state to exercise certain powers of the state, especially in the creation of authentic written evidence in the field of civil law. These powers are granted to the notary through the Notary Position Law. The authority held by a notary is an attributed authority, meaning it is directly granted by law, not through the government's organizational structure. In this context, the notary position is not part of the structural positions within the government organization, such as executive, legislative, or judicial positions. Instead, the notary holds an independent position as a public official tasked with handling civil law matters, particularly in the creation of authentic deeds and other legal documents, to serve the public.

Soegondo Notodisoerjo's opinion provides an understanding of a public official as someone who is appointed and dismissed by the government and is given authority and responsibilities to serve the public in specific matters because they participate in exercising a power derived from the government's authority. Within their role, there is an inherent characteristic and distinct feature that sets them apart from other positions in society [14].

Regarding Cyber Notary, its main function is to perform certification and authentication in electronic transaction processes. Certification itself means that a notary has the authority to act as a Certification Authority (trusted third party) so that the notary can issue digital certificates to interested parties. On the other hand, authentication function is related to legal aspects that must be fulfilled in the execution of electronic transactions [15].

The implementation of Cyber Notary based on the concept of Electronic Know Your Customer (e-KYC) using the National Identity Number (NIK) in the creation of notarial deeds in Indonesia has many benefits. Implementing e-KYC (Know Your Customer electronically) in the process of creating authentic deeds by a Notary has numerous advantages, especially in preventing identity theft and related criminal activities.

The e-KYC tool based on the NIK serves to verify the accuracy of an individual's personal data in the Civil Registry database when citizens enter their data such as name, address, place and date of birth, along with NIK verifier, fingerprint, iris scan, and facial photo in the e-ID card. Consequently, once citizens have entered their data, they cannot record new data outside of the information initially inputted.

Regarding Notaries and their attribution-based authority from Law Number 2 of 2014 concerning the Position of Notaries (hereinafter referred to as the Notary Law), they have the authority to create authentic deeds. Notaries creating authentic deeds provide a service to the community to the best of their ability. Through the deeds created by or before them, notaries carry a burden and responsibility to

ensure legal certainty for the parties involved. Therefore, there is a need for both individual and social responsibility, especially adherence to positive legal norms and a willingness to adhere to the Code of Ethics of the profession, which will strengthen existing positive legal norms.

Notaries must also carry out their duties and authority with accuracy and honesty, meaning they act in accordance with truthfulness as per their oath of office. In providing their service, a notary must uphold the noble ideals of the profession in line with the demands of conscience [16].

Conclusion

The authority of Notaries in implementing electronic Know Your Customer (e-KYC) based on the population registration number (NIK) regarding the creation of authentic deeds is still not clearly detailed. The regulations related to electronic transaction certification by Notaries (Cyber Notary) in legislation, especially the Notary Law, are incomplete or unclear due to the absence of implementing regulations related to cyber notaries. This lack of clarity is due to the incomplete understanding of the definition of the authority to certify electronic transactions. However, the ITE Law has provided more comprehensive regulations and identified who can be involved in certifying electronic transactions, including Notaries as registration authorities regulated in the Minister of Communication and Informatics Regulation as a derivative regulation of the ITE Law. The authority of Notaries to certify electronic transactions is an additional authority that arises due to technological advancements and the need for legal certainty to establish authentic evidence.

References

1. Permana A. Mengenal Sistem e-KYC: Manfaat dan Keuntungannya di Era Digital. ITB.ac.id,2022 April 13. Available from: https://www.itb.ac.id/news/read/58560/home/mengenal-sistem-e-kyc-manfaat-dan-keuntungannya-di-era-digital. Accessed February 20, 2024.
2. Kamus Besar Bahasa Indonesia (KBBI). Jakarta: PT. Gramedia Pustaka Utama, 2014.
3. Rossalina Z. Keabsahan Akta Notaris Yang Menggunakan Cyber Notary Sebagai Akta Otentik. Brawijaya Law Student,2016.
4. Nurita E. Cyber Notary Pemahaman Awal dalam Konsep Pemikiran. Bandung: Refika Aditama, 2012.
5. Shadily JM. Kamus Hukum Inggris Indonesia. Jakarta: Gramedia Utama, 2012.
6. Wignjosoebroto S. Hukum, Konsep dan Metode. Malang: Setara Press, 2013.
7. Priscyllia F. Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. Jatiswara,2019:34(4):239-249.
8. Tumalun B. Upaya Penanggulangan Kejahatan Komputer dalam Sistem Elektronik Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang Undang Nomor 11 Tahun 2008. J Lex Et Societatis,2008:6(24).
9. Gopinathan ZD. PISA and High Performing Education Systems: Explaining Singapore's Education Success. Comp Educ,2016:52(4):449-472.
10. Haque MS. Public Administration and Public Governance in. In: Pan Suk Kim, editor. Public Administration and Public Governance in ASEAN,2009. p,246-271.
11. Lam NM. Government Intervention in The Economy: A Comparative Analysis of Singapore and Hong Kong. Public Adm Dev,2006:20(5):397-421. Available from: https://www.researchgate.net/publication/241662202_Government_intervention_in_the_economy_a_comparative_analysis_of_Singapore_and_Hong_Kong
12. Chen BS. Dynamic Governance: Embedding Culture, Capabilities and Change in Singapore. Singapore: World Scientific Publishing, 2007.
13. Wei WK. Successful E-Government in Singapore. Commun ACM,2004:47(6):95-99. Available from: https://www.researchgate.net/publication/220422089_Successful_E-Government_in_Singapore
14. Notodisoerjo RS. Hukum Notariat di Indonesia Suatu Penjelasan. Jakarta: Rajawali Pers: 1982.
15. Resen RF. Keabsahan Akta Notaris Berbasis Cyber Notary Dalam Pembuatan Akta Otentik. J Kertha Desa,2022:10(2):58-69.
16. Saleh UP. The Urgency of Applying Article 39 paragraph (2) UUJN Against Prevention of Indications of Criminal Acts in Notary Deeds. J Ilmu Syariah Perundang-undangan Ekonomi Islam,2023:15(2):58-70.