CERTIFIED VERSUS UNCERTIFIED ELECTRONIC SIGNATURES: LEGAL CONSEQUENCES AND BEST PRACTICES IN INDONESIA

Farhan Hamka Ilyasa[1*], Ariawan Gunadi[2]
[1,2]Faculty of Law, Universitas Tarumanegara, Jakarta
E-mail: [1)] farhan.217222008@stu.untar.ac.id, [2)] ariawang@fh.untar.ac.id

Abstract

This article examines the legality and validity of electronic signatures in Indonesia, especially for crucial documents such as the Power of Attorney and Letters of Indemnity, in the light of digital transformation. In this study, a normative legal research method, more popularly known as doctrinal research, was employed, where an in-depth analysis of the legislative texts and available legal materials is needed to construct sound legal reasoning. Approach: The paper combines a conceptual analysis of legal principles with a statutory approach that analyzes whether there is harmony within the various legislative provisions. Various statutes and regulations in Indonesia are critically analyzed, including the Law on Electronic Information and Transactions, Government Regulation concerning the Execution of Electronic Systems and Transactions, and the Minister of Communication and Informatics Regulation on Electronic Certification. The discussion should be centered on what legal provisions must be in place for the acceptance of electronic signatures certified and those not certified. It, therefore, sets out the legal implications of the use of electronic signatures and gives comprehensive recommendations of the best practices as a means of ensuring legal certainty and legality in their implementation in Indonesia. The Journal is intended to assist businesses and lawyers to pass through those issues with ease. To this end, this journal will consider in great detail the legal framework for electronic signatures.

Keywords: *Digitalization, Electronic Certification, Electronic Signature, Electronic Transactions Law, Information*

1. INTRODUCTION

Putting a signature is among the central elements of our everyday life due to its feasibility and effectiveness. Signature fields serve quite a few important functions, which include verification of identity, assurance about the integrity of documents, allowance of amendments in letters or documents, which serves as proof of consent for changes in documents and other authentication needs (Suwignyo, 2009).

The need for a signature helps differentiate one document from another or those issued by different individuals. In simple terms, the role of a signature is to give a document an identity since verification can occur with the signature appended to any document. In this perspective, appending a signature involves writing the name of the individual, and merely appending initials, which are abridged versions of the signature, is not sufficient. The signer must handwrite the name of their own volition (Mertokusumo, 2009).

The digital transformation of business processes has become a critical focus for organizations worldwide, including in Indonesia. One significant aspect of this transformation is the adoption of electronic signatures, which offer a more efficient and streamlined method for signing documents compared to traditional handwritten signatures. This shift is particularly relevant for documents such as Power of Attorney

and Letters of Indemnity, which are frequently used in various legal and business transactions.

UNCITRAL itself has long recommended the legal recognition of electronic information and/or documents through various frameworks: the Model Law on E-Commerce in 1996, the Model Law on E-Signatures in 2001, the United Nations Convention on the Use of Electronic Communications in International Contracts in 2005, and Promoting Confidence in E-Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods in 2009 (Mayana & Santika, 2021).

The government regulates the legality of electronic signatures through several official regulations. Functionally, electronic signatures serve as tools for verifying and authenticating the identity of the signer while ensuring the integrity and authenticity of the document. Electronic signatures display the signer's identity, verified based on the unique data created for the electronic signature, which exclusively refers to the signer. Additionally, electronic signatures have advantages over manual signatures, as they can invalidate a document if any changes occur to the text or metadata of the signature. This guarantees that the document remains safeguarded against unauthorized alterations. This functionality facilitates the verification process in contrast to traditional signatures, which necessitate an extensive forensic analysis to establish their authenticity (Maurisa & Rahayu, 2021).

The regulatory framework of Indonesia, regarding electronic signatures, is primarily set by the Law on Electronic Information and Transactions, first in force in 2008 and updated further in 2016. This law creates a basic framework to carry out electronic signatures and electronic documents in pursuit of their legal acceptance and validity. Furthermore, conditions and procedures concerning electronic signatures are more specifically governed by Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions, including the Regulation of the Minister of Communication and Informatics Number 11 of 2018 on the Implementation of Electronic Certification.

Driving the usage of electronic signatures in Indonesia is mainly done to speed up the signing of documents efficiently, which is very important in industries such as logistics and container lending that rely on quick and efficient document management. This will enable organizations to save man-hours spent on documents by allowing clients to electronically sign their documents through a web-based platform and enhance overall operational efficiencies.

In any case, the shift to electronic signatures raises a plethora of legal questions and challenges. Key issues about the legal equivalence of documents signed electronically versus traditional, the exact requirements electronic documents must satisfy to be legally valid under Indonesian law, and the implications of using qualified versus unqualified electronic signatures. Issues like this need deep knowledge of the underlying legal framework and best practices while deploying electronic signatures to secure compliance with the law, as well as minimise any potential legal risk.

This journal intends to analyze the legal effects of electronic signatures in Indonesia by focusing on their application to digitalize Power of Attorney and Letters of Indemnity. The study will hence analyze the concerned laws and regulations for the purpose of providing practical insights and recommendations to businesses and legal practitioners on how best to handle the challenges that characterize the implementation of electronic signatures.

2. RESEARCH METHODS

According to Soekanto and Mamudji (2004) the legal research normative, usually named doctrinal legal research is a type of inquiry conducted to examine one or more written laws or various legal texts. The conceptual approach stems from the perspectives and doctrines that have developed within the field of law. Understanding these perspectives and doctrines provides a foundation for researchers to build legal arguments in addressing the legal issues being investigated (Marzuki, 2016). The Statue Approach involves examining all laws and regulations related to the legal issue at hand. The result of this examination is an argument that can be used to resolve the legal issue being studied (Marzuki, 2016).

This research is conducted by examining legal materials through library research or secondary data, which consists of primary legal materials, secondary legal materials, and non-legal materials. Primary legal sources include Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 19 of 2016 amending Law No. 11 of 2008 on Electronic Information and Transactions ("ITE Law"), Government Regulation No. 71 of 2019, on the Implementation of Electronic Systems and Transactions ("GR 71/2019"), and Regulation of the Minister of Communication and Informatics Number 11 of 2018 on the Implementation of Electronic Certification ("Ministry Regulation 11/2018").

Secondary legal sources are derived from various research findings published in journals. Tertiary legal sources come from other references, such as dictionaries, electronic media, and others. The statutory approach involves analyzing relevant laws related to the formulated issues. This approach examines the coherence between laws or between laws and the constitution to derive legal arguments that address the legal issues.

3. RESULTS AND DISCUSSION

3.1. Electronic Signature Documents

Signatures are a very important aspect of social interaction. This is considered to be very important because they sign to indicate agreement with something by an individual. Signatures serve four different purposes, which are: evidence, consent, executing formality and efficiency. Therefore, there is a need to have laws regulating digital signatures/electronic signatures.

An electronic signature is not a handwritten signature on paper or a scanned signature. Instead, a message digest or hash is a mathematical summary of the document sent through cyberspace (Partodihardjo, 2009). An electronic signature differs from a digital signature in that the former is a legal term defined under Indonesian regulations, while digital signatures mean a way of electronically signing with asymmetric cryptography with the help of a public key infrastructure (Cahyadi, 2020). In electronic transactions, the use of digital signatures is increasingly replacing traditional paper signatures. Digital signatures are essential for ensuring the authenticity of electronic documents (Anshori et al., 2022).

The reasons for adopting Digital Signatures are as under: It saves time because documents can be signed and sent from anywhere and at any time. It saves on costs because there is no budgeting for administrative requirements like purchasing stationery, shipping costs, storage costs, etc. Signing and sending documents can be done from any place without any extra cost, provided one has a smartphone or computer connected to

the internet. It is an eco-friendly method whereby the consumption of papers and fuels that happen in everyday life is reduced by avoiding printing and couriering of documents (Cahyadi, 2020).

The definition of an Electronic Signature based on Article 1 number 12 ITE Law concerning Information and Electronic Transactions says that "an Electronic Signature is a signature consisting of Electronic Information that is attached, associated or related to other Electronic Information used as a means of verification and authentication."

Under Article 11 of the ITE Law, an electronic signature shall be valid and legally binding, having legal consequences, provided that it meets three requirements:

a. The data used for signing the electronic signature is not solely owned exclusively by the signatory.
b. At the time of signing, the Data used for the creation of an Electronic Signature shall be, within the context of the signature, controlled only by the person who signs.
c. Any alteration to an Electronic Signature, which occurs after the time of signing is capable of being detectable.
d. Any modification to the electronic information associated with the electronic signature after the time of signing is detectable.
e. It must be possible to identify the signatory.
f. It must be possible to indicate that the signatory has consented to the electronic information being signed.

Article 60 paragraph (1) of GR 71/2019 states that electronic signatures have two main functions, namely authentication and verification of the identity of the signatory, plus integrity and authenticity in respect of the electronic information. For an electronic signature, two aspects must be met:

a. Authentication of the Electronic Signature Owner:
   This means the electronic signature truly belongs to the signer listed on the digital document.
b. Authentication of the Document:
   The digital document must also be proven authentic after being signed, ensuring its content remains the original and cannot be tampered with.

The authentication of both the signer and the document is a tool to prevent forgery and is an application of the "non-repudiation" concept in information security. Non-repudiation ensures the authenticity of the document and its delivery process, preventing the signer from denying they signed the document and the sender from denying they sent the document (Hiariej, 2013).

Based on Article 60 paragraph (2) GR 71/2019 categorizes electronic signatures into two distinct types:

a. Certified Signatures
   A certified electronic signature shall have to be conducted in respect of the stipulations on the legal validity and legal effect as referred to in Article 59 paragraph 3, using an electronic certification by Indonesian Electronic Certificate Service Providers and created by certified electronic signature creation devices.
b. Uncertified Signatures
   Uncertified electronic signatures are created without using the services of an electronic certificate provider.

Certified electronic signatures must adhere to specific legal standards to ensure their validity and enforceability. These signatures are created using certified electronic signature-making devices.

Certified electronic signatures must be issued by Indonesian Electronic Certificate Providers (PSrE Indonesia) that have been recognized and have passed audits based on standards set by the Ministry of Communication and Information Technology (Kominfo), under Article 1, point 5 of Ministry Regulation 11/2018 says an electronic certificate provider is a legal entity that acts as a trusted party, responsible for issuing and auditing electronic certificates.

Consistently, under the current statutes and regulatory schemes developed by the government, a digital signature or electronic signature must be backed by appropriate technological capabilities that guarantee adherence to set criteria. These include digital attributes or electronic signatures and verification capabilities (Budhijanto, 2017).

Legal effect arising from the usage of an authenticated electronic signature is stipulated in the ITE Law, Government Regulation on Implementation of Electronic Systems and Transactions, and by Ministry Regulation 11/2018. Laws have pointed out some subsequent legal effects of authenticated electronic signatures:

1) Validity and Legal Force:
   Certification means that an electronic signature shall be legally valid and enforceable; hence, it is legally binding.
2) Electronic Certificate:
   A certified signature shall be supported by the giving of an electronic certificate issued by an Indonesian Electronic Certification Provider. This means a certificate identifying the authenticity of a signature and the identity of the signatory.
3) Certified Device:
   When developing certified electronic signatures, aligns with using a certified device to make an electronic signature by ensuring security and integrity.

Concerning the characteristics of digital signatures and electronic signatures, a principal element is their ability to authenticate, which guarantees the legitimacy of both the digital signature and the associated digital document. Considering that digital technology enables individuals to replicate and reproduce documents as well as digital signatures, the authentication feature of digital signatures assumes significant importance (Wahyuni et al., 2022).

Certified electronic signatures using electronic certificates give the owner assurance by verifying the authenticity of the data showing the identity of the certificate holder in the electronic document. This preserves the integrity of signed electronic transactions for oversight and non-repudiation. Non-repudiation is a concept that brings the validity of the signature, hence a signer cannot deny involvement in the electronic transaction.

In contrast, an uncertified electronic signature is one generated outside of any Indonesian Electronic Certification Provider. This kind of signature maintains legal status but does not hold the same legal warranty as certified signatures and may become much weaker in situations involving courts.

The fundamental difference between certified and uncertified digital signatures lies in the validity of the data and legal certainty. The validity and legal certainty are only guaranteed through electronic certificate providers (PSrE) that are licensed by the government, specifically the Ministry of Communication and Information Technology.

The implementation of this policy means that certified electronic signatures can serve as a solution for ensuring the legality of documents in the digital era. It is further reportedly said that an electronic signature is not only safe and easy but also legally valid and has the same effect as a conventional manual signature, provided it meets the requirements outlined in Article 11 of Law No. 19 of 2016, amending Law No. 11 of 2008 on Electronic Information and Transactions.

3.2. Requirements To Make An E-Document Valid Under Indonesian Law

To ensure the validity of an electronic document under Indonesian law, specific procedures and criteria must be met as outlined in the Regulation of the Minister of Communication and Informatics concerning the Implementation of Electronic Certification. Firstly, applicants must apply for the issuance of an Electronic Certificate through an Electronic Certification Organizer. For corporate applications, a corporate taxpayer identity card is required. Once the verification process is completed, the applicant receives an account to download the Electronic Certificate issued by PSrE Indonesia. In the Ministry Regulation 11/2018, the ways that can be done are as follows:

a. According to Article 25 Ministry Regulation 11/2018 The applicant can apply for the issuance of an Electronic Certificate to the Electronic Certification Organizer.
b. According to Article 32 Ministry Regulation 11/2018 Applications for corporations must use a corporate taxpayer identity card
c. Upon verification, applicants will be given an account that will allow them to download the Electronic Certificate issued by PSrE Indonesia. This account also provides a facility for administration to be given by each PSrE for services such as certified signature, certified Electronic Seal replacing corporate stamps, and various other services.

Article 11 Paragraph 1 of the ITE Law stipulates that an electronic signature is valid and legally binding if the following are realized:

a. electronic signature creation data are related only to the Signatory;
b. All information about the making of an Electronic Signature within the context of an electronic signature procedure is to be considered strictly the personal affair of the Signatory.
c. Any alteration to the Electronic Signature that occurs after the time of signing is detectable;
d. Any changes to the Electronic Information associated with the Electronic Signature after the time the document was signed can be detected;
e. There are certain ways in which to identify who the Signatory is; and
f. There are specific modes of indicating that the Signatory accepted the relevant Electronic Information.

Article 11 paragraph 1 of the ITE Law provided that an electronic signature shall have legal validity and, as a consequence, legal effects only in case certain requirements are met. Such requirements include the authenticity of a signature authentication, integrity both of a signature and of a document to which it relates not being altered after signing, and non-repudiation impossibility of a signing party to deny the performance of such signing.

Government Regulation concerning the Implementation of Electronic Systems and Transactions stipulates that an electronic signature shall be sufficient as a means for the authentication and validation of the identity of the signer to ensure the integrity and

authenticity of Electronic Information. Under Government Regulation on the Implementation of Electronic Systems and Transactions, it is mentioned that for Indonesian electronic certification, the establishment of the electronic transaction systems must obtain approval from the relevant Minister and meet the recognition stipulated in the Ministerial Regulation concerned. Recognition of the establishment of electronic transaction systems shall be based on the Regulation of the Minister of Communication and Informatics on the Implementation of Electronic Certification.

The validity of the application of electronic signature techniques is also dependent on the utilization of an electronic system that adheres to Indonesian laws. Electronic evidence, in this case electronic signatures, shall be considered expressive, even though it is ensured that the entire information is governed, it is auditable, retrievable and can be presented for an explanation of the situation.

When considering electronic transactions, one crucial point that must be addressed is the effectiveness of digital signatures, which are intended to make documents or results in an electronic transaction permissible. In this context, the ITE Laws govern the verification of rights and duties contained in an electronically signed paper (Raharjo, 2005).

One crucial aspect of electronic transactions is the use of digital signatures to legalize documents or outcomes within such transactions. ITE Law addresses the authentication of rights and obligations in digitally signed documents.

Legal Impact If the Government does not verify Electronic Signatures under the ITE Law, the use of Electronic Signatures that are not certified by the Government remains valid because it does not violate the provisions of Article 11 paragraph (1) of ITE Law. The consequence is that if there is a legal problem, electronic signatures that are not certified by the Government the elements of proof at trial do not have sufficiently strong evidence.

4. CONCLUSION

Indonesian law provides a broad base for the use of electronic signatures with legality and enforceability. In the country, this is substantially regulated by the ITE Law, Government Regulation 71 of 2019, and Ministry Regulation 11 of 2018, which distinguishes between certified and uncertified electronic signatures.

Certified electronic signatures, using certified devices and having their validity checked by Indonesian Electronic Certification Providers, indeed provide very high legal certainty. They will meet the severe requirements of legal force and validity that include an electronic certificate and a certified signature creation tool. The authenticity and integrity of an electronic document are guaranteed, with non-repudiation, by this form of signature, which makes them very reliable in legal contexts.

Where uncertified electronic signatures are legally valid, nonetheless, they provide a lower level of legal surety and may be less effective in legal disputes due to their nature of not being certified. The difference between certified and uncertified signatures has brought attention to the need for using a certified electronic signature on key documents to ascertain regulatory compliance and reduce potential legal liability.

In other words, electronic signatures are indeed supported in the legal setting of Indonesia, but certified electronic signatures boast the highest legality certainty therein. It is recommended that enterprises and legal professionals apply certified electronic

signatures to ensure the validity and legal enforceability of their electronic documents and thus raise legal security with a higher degree of operational efficiency in the digital era.

REFERENCES

Anshori, I., Rahmi, E., & Syamsir, S. (2022). Polemik Penerapan Tanda Tangan Elektronik Dalam Pembuatan Akta Otentik. Recital Review, 4(2), 353–373.

Budhijanto, D. (2017). Revolusi cyberlaw Indonesia: pembaruan dan revisi Undang-Undang Informasi dan Transaksi Elektronik 2016. PT Refika Aditama.

Cahyadi, T. N. (2020). Aspek Hukum Pemanfaatan Digital Signature Dalam Meningkatkan Efisiensi, Akses Dan Kualitas Fintech Syariah. Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 9(2), 219.

Hiariej, E. O. S. (2013). Teori dan hukum pembuktian.

Marzuki, P. M. (2016). Legal Research, Revision. Jakarta: Kencana Pranada Media Group.

Maurisa, K. Z. A., & Rahayu, W. P. (2021). Meningkatkan Kemandirian dan Hasil Belajar Siswa Melalui Pengembangan Mobile Learning Berbasis Android Berbantuan Ispring Suite 9. Jurnal Ekonomi, Bisnis Dan Pendidikan, 1(6), 546–558. https://doi.org/10.17977/um066v1i62021p546-558

Mayana, R. F., & Santika, T. (2021). Legalitas tanda tangan elektronik: posibilitas dan tantangan notary digitalization di Indonesia. ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan, 4(2), 244–262.

Mertokusumo, S. (2009). Hukum acara perdata Indonesia.

Partodihardjo, S. (2009). Tanya jawab sekitar Undang-Undang no. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik: dilengkapi dalam bentuk pointers. PT Gramedia Pustaka Utama.

Raharjo, I. S. (2005). Informasi Elektronik pada Electronic-Commerce dalam Hukum Pembuktian Perdata. Universitas Airlangga.

Soekanto, S., & Mamudji, S. (2004). Penelitian hukum normative. Jakarta: PT. Raja Grafindo Persada.

Suwignyo, H. (2009). Keabsahan Cap Jempol sebagai Pengganti Tanda Tangan dalam Pembuatan Akta Otentik. Notarius, 1(1), 63–74.

Wahyuni, E., Rahman, S., & Risma, A. (2022). Keabsahan Digital Signature/Tanda tangan Elektronik Dinjau Dalam Perspektif Hukum Perdata dan UU ITE. Journal of Lex Generalis (JLG), 3(5), 1082–1098.

Copyrights