International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Law on Electronic Signatures and Orientations for Refinement in Vietnam Today[1]

Dr. Nguyen Thi Huong

Institute of State and Law, 27 Tran Xuan Soan Street, Hanoi
Email: *nguyenhuong1285[at]gmail.com*

Abstract: ***In the context of vigorous globalization and digital transformation, the study of electronic signatures has become an inevitable necessity to meet the practical demands of modern society. This article endeavors to elucidate various issues concerning electronic signatures as stipulated by current Vietnamese law, thereby establishing orientations for their refinement within the present context.***

Keywords: Electronic signature, refinement, law

1. Statement of the Problem

Signatures or other forms of authentication, such as fingerprints, are considered means to establish the identity of parties entering into an agreement and serve as a basis to bind them to the contents of a document. In current legal practice, a handwritten signature is the most prevalent form of authentication, particularly in civil transactions established in written form. A handwritten signature is typically understood as the personal identifier of the authorized representative of a party in a contractual relationship, and simultaneously represents the expression of consent and a commitment to fulfill the agreed-upon terms. In the context of the digital transformation and the robust development of information technology, the issue of electronic signatures has garnered significant attention not only from technology professionals but also from legislators. Many nations have officially recognized the legal validity of electronic signatures by enacting specific laws or amending existing regulations to conform to this novel type of signature. In essence, an electronic signature is generated through the combination of the signatory's private cryptographic key and the data requiring encryption, utilizing modern digital technology solutions, thereby aiming to verify the identity of the signatory. The advent of electronic signatures has introduced a new authentication method, contributing to enhanced efficiency and security in electronic transactions.

2. General Overview of Electronic Signatures

The matter of signatures has attracted considerable attention from numerous specialized technical organizations as well as legislative bodies. Many nations have acknowledged electronic signatures and have either codified them into distinct laws or appended provisions pertaining to this new form of signature. An electronic signature constitutes a composite of a private cryptographic key and data requiring encryption through digital technology. With the advent of electronic signatures (also known as digital signatures), a novel method for contracting parties to execute documents has emerged. A signature serves as a prevalent means to attest to the authenticity of information contained within a document. Signatures possess two principal characteristics: they serve to identify the author of the document, and they signify the author's assent to the information contained therein.

In the current digital era, signatures are not confined to paper documents but are also required to exist on a distinct type of document: electronic documents. With digital transformation encompassing all sectors, including societal life and state administration, the restricted use of electronic signatures is no longer appropriate for electronic transactions; hence, the imperative arises for signatures themselves to be "digitized". Therefore, the advent of electronic signatures marks a new stride in demonstrating the authenticity and intent of contracting parties in online transactions. The UNCITRAL Model Law on E-Signatures 2001 (UNCITRAL Model Law on E-Signature) defines an electronic signature as "data in electronic form affixed to or logically associated with a data message and used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message" (Article 2, paragraph (a) of the UNCITRAL Model Law on E-Signatures).

To distinguish it from a traditional signature, an electronic signature possesses the following distinct characteristics:

Firstly, the manifestations of electronic signatures are highly diverse. Electronic signatures can appear in basic forms such as: a signature line or an image of a signature placed at the end of an email; an "I agree" checkbox or a registration click-button on digital service platforms; the input of personal information (full name, address, phone number, bank account number), entering an OTP verification code sent to a phone number, etc. Besides, electronic signatures also encompass other complex forms necessitating the intervention of technology and engineering, such as: digital signatures employing a two-key system based on asymmetric encryption, USB Tokens, and the use of remote electronic signatures with specialized hardware integrated into computer devices (HSMs), etc.

Secondly, electronic signatures necessitate numerous supporting technical conditions. Specifically, to

[1] This research is the product of a Ministry-level project: *"Review of the Implementation of the Civil Code 2015"*, led by Dr. Nguyen Thi Huong.

fundamentally facilitate the application of electronic signatures, agencies and organizations must invest substantially in the development of network infrastructure, power systems, the establishment of advanced database systems, and the deployment of hardware for storing electronic signatures. Additionally, electronic signatures also demand a high level of expertise in information technology applications, as well as profound knowledge in electronics, telecommunications, and information technology itself, etc. Specially, network infrastructure must be developed at both ends, encompassing both the sender and the receiver of the message. Should there be an asymmetry in technological infrastructure, the utilization of electronic signatures would become exceedingly challenging.

Thirdly, an electronic signature possesses the capabilities of authentication and certification. Indeed, an electronic signature serves as a reliable basis for authenticating the signatory as well as the content of the data message, and it signifies the intent to establish a transaction on a cloud-based platform, especially when the parties to the transaction are unable to negotiate directly with each other.

Fourthly, the legal validity of electronic signatures has been widely recognized as equivalent to that of handwritten signatures in numerous nations. The legal validity of electronic signatures is acknowledged by countries and stipulated either in Laws on E-commerce or in specialized statutes concerning electronic signatures (as per the EU Directive on electronic signatures dated December 13th, 1999, and the Electronic Signatures in Global and National Commerce Act of 2000 (E-Sign Act) of the United States, along with provisions found in national and international commercial law on signatures (referencing FTU Working Paper Series, Vol. 1 No. 5 (05/2022), p. 79), all deem electronic signatures to be of equivalent value to handwritten signatures in traditional transactional documents).

The utilization of electronic signatures offers the following advantages:

Firstly, using electronic signatures is a prerequisite for ensuring the legal validity of electronic commerce transactions, enabling these transactions to be conducted in an electronic environment. Unlike traditional written contracts bearing handwritten signatures, electronic commerce contracts utilizing electronic signatures are transmitted via the internet in an exceptionally brief period. Thus, the use of electronic signatures contributes to time savings and increased efficiency in transactions.

Secondly, electronic signatures can mitigate signature forgery (in the sense of creating an electronic signature identical to one currently in use, verifiable conventionally via a public key).

Thirdly, electronic signatures prevent the potential for document falsification. Electronic documents pertaining to e-commerce, once signed with a digital signature, cannot be altered. When the document's content is modified, the public key will no longer be compatible with the private key; thus, the recipient will be unable to use the public key to verify the document's integrity and authenticity. Therefore, the electronic signature can be regarded as a tool for identifying the author of an electronic document as well as for ensuring the integrity of the text, serving as a legal basis to protect the legitimate rights and interests of the parties involved in the transaction. One of the crucial elements for ensuring the authenticity of a contract within an electronic environment is the electronic signature.

3. Overview of the Law on Electronic Signatures in Vietnam Currently

In Vietnam, the legal basis for electronic signatures was first established in the Electronic Transactions Law 2005, as the inaugural legislation regulating transactions in the digital environment. This Law was subsequently amended and replaced by the Electronic Transactions Law 2023 to ensure synchronization with the trend of digital technology development. Furthermore, the system of guiding implementation documents related to electronic signatures includes: Decree No. 130/2018/ND-CP dated September 27th, 2018, of the Government, detailing the implementation of the Electronic Transactions Law regarding digital signatures and digital signature certification services; Circular No. 16/2019/TT-BTTTT dated December 5th, 2019, of the Ministry of Information and Communications, providing guidance on technical requirements and standards applicable to digital signatures; and Decree No. 23/2025/ND-CP dated February 21, 2025, regulating electronic signatures and trusted services. Besides, foundational provisions in documents such as the Civil Code 2015, Commercial Law 2005, Information Technology Law 2006, and several other legal instruments also provide the basis for deploying the electronic signature system, establishing digital signature certification service providers, and defining the legal validity of electronic signatures in civil transactions.

Compared to the Electronic Transactions Law 2005, the Electronic Transactions Law 2023 has introduced lots of revisions and significant amendments related to electronic signatures:

First, regarding concepts: Clause 11, Article 3 of the Electronic Transactions Law 2023 has updated and added a series of new concepts that were not specifically regulated before, such as electronic signature, digital signature, timestamp, digital data, master data, electronic environment, digital signature certification service, etc.

Second, regarding the conditions for a digital signature to be recognized as an electronic signature: Clause 3, Article 22 of the Electronic Transactions Law 2023 specifies that a digital signature shall be deemed an electronic signature if it fully satisfies the legal requirements in the conditional business sector related to electronic transactions, encompassing three types of services: timestamp issuance service, data message certification service, and public digital signature service. This significantly expands upon the Electronic Transactions Law 2005, which only referred to electronic signature certification service.

Third, regarding technology and security: The Electronic Transactions Law 2023 emphasizes requirements for verifying the signatory's identity, affirming the signatory's

consent to the content of the data message, stipulating that signature creation data must be under the sole control of the signatory at the time of signing, and concurrently ensuring that any alterations occurring after the time of signing can be detected.

Fourth, regarding the classification of electronic signatures: Article 22 of the Electronic Transactions Law 2023 has formally classified electronic signatures into three primary categories: specialized electronic signatures, public digital signatures, and specialized digital signatures used in official duties. This is a new regulation of great practical significance, creating favorable conditions for businesses to flexibly apply electronic signatures to commercial contract conclusion activities in the coming time.

However, despite the Electronic Transactions Law 2023 expanding its scope of regulation compared to the 2005 Law, certain limitations still exist in the application of electronic signatures. Primarily, the scope of application of the Electronic Transactions Law will remain confined to "transactions", meaning it encompasses contracts or unilateral legal acts expressing the will of the parties. Thus, general administrative procedures for the populace in society will not yet have a legal basis to apply electronic signatures at the scale of an overarching law, being, at most, limited to specific, fragmented areas. Furthermore, some specialized sectors still necessitate traditional forms to ensure authenticity, prevent fraud, and protect the rights and interests of participating parties, including transactions related to land use rights and housing ownership rights, such as contracts for sale, transfer, donation, and mortgage, which require notarized or authenticated written documents in accordance with the Land Law 2024 and Housing Law 2023. This inconsistency creates difficulties in the widespread deployment of electronic signatures, reducing the efficiency of inter-sectoral electronic transactions, particularly in administrative, civil, and commercial procedures. This necessitates further review and synchronized amendment of the legal system to ensure consistency and alignment with the national digital transformation trend.

Among various types of electronic signatures, digital signatures are considered the most prevalent form. Essentially, a digital signature is a data message, a type of electronic signature that offers high security and is widely utilized. The formula for generating a digital signature depends on three input factors: the electronic document to be signed, the private key, and the digital signing software. Digital signatures are based on the theory of cryptography and asymmetric encryption algorithms. The acknowledgment of a digital signature as belonging to a specific agency or individual must be provided by a certification service provider, and this organization must be recognized for its legal and technical standing[2]. Nevertheless, digital signatures are intrinsically linked to digital signature certificates issued by a certification service provider, which have a defined validity period, typically ranging from 1 to 3 years. This presents a potential risk: after the certificate expires or is revoked, the signature verification software cannot authenticate the validity of the digital signature accompanying previously signed documents. This means that an electronic transaction, though legally signed at a past date, may subsequently lack sufficient legal evidence, potentially leading to it being deemed illegal should a dispute arise[3].

Moreover, while the Electronic Transactions Law 2023 has categorized electronic signatures, it does not address or acknowledge whether scanned signatures or image-based signatures can be considered electronic signatures. Although not regulated by the Electronic Transactions Law, in practice, scanned and image-based signatures are commonly used in numerous commercial contracts between Vietnamese enterprises and foreign partners. Consequently, the incompleteness of the Law's provisions creates legal risks pertaining to the form of confirmation in these contracts should disputes arise. According to the perspective of the Drafting Committee of the Electronic Transactions Law 2023, other forms of electronic confirmation, such as scanned signatures, image-based signatures, one-time passwords (OTP), and text messages (SMS), etc. are not electronic signatures[4]. Nevertheless, to align with practical implementation in certain sectors such as banking and customs, and to promote electronic transactions, Clause 4, Article 22 of the Electronic Transactions Law 2023 has additionally stipulated that the use of these forms of confirmation shall be carried out in accordance with relevant legal provisions.

The Electronic Transactions Law 2023 has demonstrated a lack of stringency in its regulations concerning electronic signatures by leaving open the recognition of the legality of commonly used electronic signature types, thereby creating a legal void in ensuring the voluntary nature of the signatory when entering into electronic contracts. This, in turn, reduces safety and increases risks for parties in electronic transactions in many real-world scenarios, such as: one party denying the attachment of their signature image to a contract or disclaiming the use of a digital signature account to conclude a contract; a buyer/service user easily clicking the pre-installed 'agree' button due to its convenience without clearly understanding the legal consequences of this action or implicitly agreeing to any changes in contract terms; or contracts lacking validity because widely used signature types are not yet governed by legal provisions[5].

Although electronic signatures have seen immense development and advancement in recent years, the current reality indicates that electronic signatures are not yet perfected or widely utilized in societal life. This stems from users' apprehension towards employing electronic signatures

[2] Truong Thi Nho, *Perfecting Vietnam's law on digital signatures*, accessed on September 23rd, 2025 at: https://hcmussh.edu.vn/news/item/17556.

[3] Nguyen Thi Long, *Perfecting Vietnam's legal regulations on electronic signatures*, 2022, Journal of Democracy and Law No. 6/2022, p.35.

[4] Nguyen Manh Tung, *The Law on Electronic Signatures in Commercial Contracts – Reality and Recommendations*, 2023, Master's Thesis, University of Banking Ho Chi Minh City, p. 46.

[5] Tran Thien Trang, *The legality of electronic signatures in electronic contracts: The experience of the European Union and the United States - Recommendation for completion*, Journal of Industry and Trade - Results of scientific research and technology application, No. 13 June 2024.

in high-value transactions, due to concerns about their security and safety. This persists despite modern technologies making the infringement or forgery of high-tech electronic signature types almost impossible and inherently safer than conventional signatures. Due to limited knowledge and insufficient dissemination regarding electronic signatures, users feel apprehensive about the advanced technological concepts these signatures employ and, consequently, tend to avoid adopting this type of signature. Coupled with imprecise regulations concerning other forms of electronic signatures that primarily focus on digital signatures, small, individual entities face greater difficulty and anxiety in using common types of electronic signatures, thereby hindering the broader adoption of electronic signatures.

4. Orientations for Perfecting the Law on Electronic Signatures in Vietnam Currently

Firstly, an electronic contract is an agreement between two or more parties to establish or terminate a legal relationship, expressed in electronic form. Consequently, the act of electronic signing gives rise to numerous legal issues, particularly concerning the validity of the signature on electronic contracts, as well as the voluntariness and genuine intent of the parties involved in the transaction. Therefore, based on referring to the provisions from eIDAS of the European Union, Vietnamese law needs clear and specific regulations regarding the recognition or non-recognition of various types of electronic signatures currently existing in the e-commerce environment, as well as clarifying the legal consequences when the type of signature used does not meet legal conditions. Furthermore, it is necessary to supplement regulations on the requirements and conditions applicable to electronic signatures in general, including specific signing methods, instead of solely focusing on digital signatures as is currently the case. This is to ensure effectiveness in protecting the legitimate rights and interests of parties entering into electronic contracts, not only through elements such as confidentiality, identification, non-repudiation, and information integrity, but also to promptly reflect the diverse development of electronic signature and electronic contract forms today.

Secondly, the principle of accepting the validity of a signature at the time of signing must be stipulated, specifically that *"an electronic signature possesses legal validity if, at the time of signing, the digital certificate remains effective and the signing is legitimate"*. Simultaneously, legal provisions also need to be supplemented regarding the issue of storing authentication evidence, whereby it must be mandatory to retain records of the timestamp and the certificate's validity status at the moment of signing, as well as permitting the use of electronic evidence storage services to preserve the signature's value. Lawmakers may consider the feasibility of TrustCA Timestamp, which is a technology offering the highest value in combating fraud and forgery in electronic transactions, ensuring legal certainty for long-term electronic document storage, long-term document authentication, and reliability even after digital certificates expire. This technology facilitates a complete replacement of paper copies, eliminating the need for printing and substituting paper archives with electronic ones. The application of timestamped digital signatures and digital signatures compliant with long-term digital signature standards LTV/LTANS also aids in authenticating electronic documents independently of the digital certificate's validity period or certificate revocation orders, thereby ensuring full compliance with regulations on long-term authenticated electronic document storage under Vietnamese and international law.

Thirdly, it is imperative to acknowledge the mandatory implementation of multi-factor authentication for electronic signatures in certain specific cases. In many current systems, electronic signatures – particularly digital signatures – only require a single authentication step (typically a password or USB token). This poses numerous risks, such as the possibility of unauthorized individuals gaining access and executing fraudulent signings if they acquire the device and PIN; concurrently, it complicates the determination of responsibility in the event of disputes and increases the risk of information theft or misuse within the inherently insecure internet environment. In an era of increasingly sophisticated cybercrime, relying solely on a single authentication factor is insufficient to guarantee the integrity and security of electronic transactions. Therefore, the author proposes mandatory multi-factor authentication for electronic signatures utilized in high-value contracts of VND 500,000,000 or more; financial-banking transactions; or the signing of state administrative documents.

Fourthly, there is a need for regulations to standardize the use of digitally signed electronic data with provisions on notarization and certification. A digitally signed data message that meets the stipulated security conditions possesses legal validity akin to an original. However, currently, there are no specific regulations concerning what constitutes an "original", a "copy", or the legal validity of a copy of a digitally signed data message. A digitally signed data message is stored and transmitted electronically. It can be understood that the original of a digitally signed data message is the one created and stored on the originating device, while a copy of this data message is a duplicated and transmitted version. For conventional electronic data, the issue is ensuring the integrity of the transmitted data, preventing any alteration from the initial original. Conversely, for digitally signed electronic data, data integrity is resolved through the reliable authentication function of the digital signature. Therefore, with digitally signed data, there is no distinction between an original and a copy, as inherently, only one version is required, and even if multiple copies are made, these copies remain identical without any changes or differences. As a result, issuing copies from an original or certifying copies from a master document will be meaningless for digitally signed documents. Accordingly, it is necessary to supplement regulations on the original, copy, and legal validity of electronic data copies to provide a clearer basis for the use of digitally signed electronic data, thereby avoiding unnecessary obstacles arising from regulations applicable to paper documents and traditional signatures.

5. Conclusion

As the international business landscape gradually enters a phase of digital transformation amidst the pressures of the pandemic, electronic transactions are becoming increasingly common. Consequently, the legal validity of electronic transactions and electronic signatures has become a concern for businesses. In practice, although digital signatures are the most widely used and common type, the intent of parties when concluding contracts using other types of electronic signatures should also be recognized and assured of legal validity. Vietnamese law on electronic transactions still lacks specific provisions regarding non-digital electronic signatures, thus making the implementation and application of the law in general, and the use of electronic signatures in particular, more challenging. In light of this situation, Vietnam should amend and particularize the provisions of the Law on Electronic Transactions to stipulate multiple tiers of signatures, similar to the regulations of the European Union, and specifically define the legal validity of each type. This would make Vietnamese law on electronic signatures consistent with international standards, thereby mitigating the risk of electronic signatures becoming insecure when businesses engage in international commerce.

References

[1] Ministry of Information and Communications (2023). *Report on the Application and Development of Digital Signatures in Vietnam in 2023*. Information and Communications Publisher.
[2] Vietnam E-commerce Association (2023). *Vietnam E-commerce Index Report 2023 – Towards Sustainable E-commerce Development*. Accessed at: https://vecom.vn/bao-cao-ebi-2023.
[3] Nguyen Manh Tung, *The Law on Electronic Signatures in Commercial Contracts – Reality and Recommendations*, 2023, Master's Thesis, University of Banking Ho Chi Minh City.
[4] Nguyen Thi Long, *Perfecting Vietnam's legal regulations on electronic signatures*, 2022, Journal of Democracy and Law No. 6/2022.
[5] Nhi Anh (2023). *Only 5% of bank customers are currently using digital signatures*. Accessed at: https://vneconomy.vn/moi-co-5-khach-hang-cac-ngan-hang-dang-dung-chu-ky-so.htm.
[6] Tran Thien Trang, *The legality of electronic signatures in electronic contracts: The experience of the European Union and the United States - Recommendation for completion*, Journal of Industry and Trade - Results of scientific research and technology application, No. 13 June 2024.
[7] Shopee Vietnam Help Center (March 2024). Terms of Service. Accessed at: https://help.shopee.vn/portal/4/article/77243.
[8] Truong Thi Nho, *Perfecting Vietnam's law on digital signatures*, accessed at: https://hcmussh.edu.vn/news/item/17556.