VOLUME 3 | NUMBER 3 | MAY 2021
Available online at http://proceedings.worldconference.id.
ISSN: 2656-1174 (online)

Legal Aspects of Electronic Signatures in E- Commerce Transactions

Enny Agustina , Muhamad Adystia Sunggara
College of Law Pertiba Pangkalpinang
ennyagustinadua@yahoo.com , dr.m.adystiasunggara@gmail.com

Abstract

Technological advances have brought about significant changes from the use of the Internet in human life. However, there are still many parties who do not understand how the position of electronic signatures that meet the requirements and standards, especially in financial technology transactions where the electronic signature function was essential. This study discusses the position of electronic signatures in financial technology transactions as well as legal remedies that can be taken if there was an electronic signature dispute. The type of research used in this paper was normative. The approach to the problem used in the writing of this research was the statute approach and the conceptual approach. The legal materials used in the writing of this study consist of primary legal materials, secondary legal materials, and tertiary legal materials. The analysis used in the writing of this research is descriptive qualitative. The conclusion in this study is that in accordance with applicable laws and regulations, electronic signatures must meet aspects ofs authenticity, integrity, and non-repudiation. With regard to fraud that causes losses to users of financial technology transactions, financial technology operators are liable for an error with a reversal of the burden of proof. Legal recognition in applicable laws and regulations confirms that electronic signatures can be used as evidence in court examinations. Legal remedies that can be taken if there is a dispute are through Litigation or Non-Litigation. The majority of business players prefer Non-Litigation legal remedies, namely alternative dispute resolution to resolve any problems that arise in business activities because the settlement system is more effective, fair, does not take up time, and is relatively cheaper.

Keywords
electronic signature, e-commerce, legal aspects.

1. Introduction

The current technological development is so fast and encourages the development of electronic trading activities (e-commerce) in Indonesia. In trading transactions conducted via the internet or cyberspace, the signature used is also a signature in the form of electronic data (electronic signature). (Harahap, 2004)

Electronic signature (digital signature or electronic signature) is not a digitized image of handwritten or not a signature or image, but is by making a message digest in advance, in the form of a mathematical summary document that will be sent via cyber space. Referring to the ITE Law Article 1 point 12, an electronic signature is a signature consisting of electronic information that is embedded, associated or related to other electronic information that is used as a means of verification and authentication. Many people are unfamiliar with the term electronic signature and think that an electronic signature is the result of a printed document that has been signed and is in soft copy. In fact, the actual electronic signature is not obtained through this method.

In order to face the era of e-commerce that is growing rapidly around the world, especially financial technology activities, business actors and all parties related to financial technology activities need to understand how the electronic signature requirements and their function in financial technology actually are. If the use of an electronic signature meets the required standards, its function can be optimized in anticipating legal risks in financial technology transactions. Especially in the financial technology of loans, financing, and provision of capital whose transaction characteristics are customer to customer (C2C), electronic signatures need to be used as an implementation of the precautionary principle.

1.1. Problems

5. What was the position of the electronic signature in financial technology transactions?
6. What legal remedies can be taken if there was an electronic signature dispute?

2. Reaserch Methodology

This research is written with the type of normative legal research, namely by explaining a problem using various legal provisions related to the problem. This legal research is based on the author's logical thinking followed by a review of applicable laws and regulations relevant to the formulation of the problem. This research,

namely the position of electronic signatures in financial technology transactions and legal remedies that can be taken if there is an electronic signature dispute. Apart from the use of statutory regulations, there is also literature that is relevant to the formulation of the problem. Literatures containing the opinions of jurists and developing doctrines in the science of law will be examined in depth to get the conclusions of this research. The approach to the problem used in this study is the conceptual approach and statute approach.

3. Result and Discussion

3.1. Position of Electronic Signature in Financial Technology Transactions

The position of electronic signatures in electronic transactions in the prevailing laws and regulations confirms that electronic signatures can be used as evidence in court examinations. The use of information technology based on electronic means in electronic transactions is believed to have a positive impact on business people, especially in terms of speed and ease of conducting transactions in global interactions without limitation of place and time. In this regard, the need for confidentiality of information and safeguarding the authenticity of information has increased so that the Government of the Republic of Indonesia issued Law Number 11 of 2008 concerning Electronic Information and Technology (hereinafter referred to as Law 11/2008) (Forder, 2008).

One of the things that need to be considered in electronic transactions is the implementation of a digital signature which aims to legalize documents / results in an electronic transaction. Related to this, Law 11/2008 regulates the authentication of rights and obligations in an electronic document that is digital signature.

3.1.1. Digital Signature

Based on Article 1 paragraph (12) of Law Number 11 Year 2008, an electronic signature is a signature consisting of electronic information that is embedded, associated or related to other Electronic Information which is used as a verification and authentication tool. Further provisions on electronic signatures are regulated by Government Regulation Number 82 of 2012 concerning Electronic Systems and Transactions (hereinafter referred to as PP Number 82 of 2012). Article 52 paragraph (2) of Government Regulation Number 82 of 2012 states that the Electronic Signature in Electronic Transactions is the approval of the Signer for Electronic Information and / or Electronic Documents signed with the Electronic Signature.

Based on Article 54 paragraph (1) Government Regulation Number 82 of 2012 Electronic Signatures are divided into 2 (two), namely:

1. Certified Electronic Signature, which is made using the services of an electronic certification operator, and proven by an Electronic Certificate; and
2. Electronic Signature is not certified, which is made without using the services of an electronic certification provider.

3.1.2. Electronic Signature Creation

Referring to Article 55 paragraph (3) of Government Regulation Number 82 of 2012, making electronic signatures must meet the following conditions:

1. The entire manufacturing process is guaranteed its security and confidentiality;
2. Electronic Signature Creation data using cryptographic codes must not be easily known from the Electronic Signature verification data through certain calculations, within a certain period of time, and with a reasonable means;
3. Electronic Signature Creation data is stored in an electronic media which is under the control of the Signer;
4. Data related to the Signer must be stored in a place or data storage facility, which uses a trusted system that can detect changes and meet the following requirements:
5. Only authorized persons can enter new data, change, exchange, or replace data;
6. Signer identity information can be checked for authenticity; and
7. Other technical changes that violate security requirements can be detected or discovered.

Every person involved in an Electronic Signature is obliged to provide security for the Electronic Signature that is used. Electronic Signature Safeguarding includes at least (Article 12 paragraph (1) Law Number 11 Year 2008).

3.1.3. The system cannot be accessed by unauthorized people

Signers must apply the precautionary principle to avoid unauthorized use of data related to Electronic Signature creation. The Signer must without delay, use the recommended method or other appropriate means and should immediately notify someone whom the Signer deems to trust the Electronic Signature or to a party supporting the Electronic Signature service if:

1. The Signer is aware that the Electronic Signature creation data has been compromised; or

2. Circumstances that are known to the Signer could create significant risks, possibly as a result of the breakdown of the Electronic Signature creation data;
3. In the event that an Electronic Certificate is used to support an Electronic Signature, the Signer must ensure the truth and integrity of all information related to the Electronic Certificate.

Before the Electronic Signature is used, the Electronic Signature Operator is obliged to ensure the initial identification of the Signer by means of (Article 58 paragraph (1) Government Regulation Number 82 of 2012)

1. Signer conveys identity to the Electronic Signature Operator;
2. Signers register with Providers or Supporters of Electronic Signature Services.

3.1.4. Electronic Signing Mechanism

Electronic Information to be signed must be known and understood by the Signer. (Article 56 paragraph (2) Government Regulation Number 82 Year 2012) Signer Approval of Electronic Information to be signed with Electronic Signature must use affirmation mechanisms and / or other mechanisms that show the intent and purpose of the Signer to be bound in an Electronic Transaction (Article 56 paragraph (2) Government Regulation Number 82 of 2012). Electronic Signatures to prove the identity of the Signers electronically are required to apply a combination of at least 2 (two) authentication factors (Article 58 paragraph (2) Government Regulation Number 82 of 2012).

3.1.5. The Power of Digital Signature Law

Referring to Article 5 paragraph (1) of Law Number 11 Year 2008, Electronic information and / or Electronic Documents and / or their printouts are valid legal evidence, this is an extension of valid evidence in accordance with the applicable procedural law in Indonesia

Based on Article 11 paragraph (1) of Law Number 11 Year 2008 jo. Article 53 paragraph (2) Government Regulation Number 82 Year 2012, Digital Signature has legal force and legal consequences as long as it meets the following requirements:

1. The electronic signature creation data is related only to the signer.
2. The electronic signature creation data during the electronic signing process is only in the power of the signing.
3. Any changes to the electronic signature that occur after the signing time can be known.
4. Any changes to electronic information related to the electronic signature after the signing time can be known.
5. There are certain methods used to identify who the signatories are.
6. There are certain ways to show that the signer has given consent to the related electronic information.

Based on the things that have been stated above, the Implementation of Electronic Transactions, especially electronic signatures in Insurance Companies against Losses, is one of the supporting factors for business transactions realized with a Digital Policy. The application of a Digital Policy in electronic transactions can be applied as long as the issuance of a digital policy has gone through a series of processes in accordance with the company's internal policies which have been standardized into the system and its security is guaranteed. (Susanti Adi Nugroho, 2018).

3.2. Legal Remedies That Can Be Found If There Are Electronic Signature Disputes

In general, e-commerce means conducting trade using electronic means. Furthermore, Electronic commerce can be defined as commercial activities carried out through the exchange of information created, stored, or communicated through electronic, optical, or analog media, including EDI (Electronic Data Interchange), E-mail, and so on. Furthermore, based on the UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 it is stated that: (Hill, 1996)

The term “commercial” should be given a wide interpretation so as to cover matters arising from all relationship of a commercial nature wether contractual or not. Relationships of a commercial nature include, but are not limited to the following transactions: any trade transaction for the supply or exchange of gods and services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitiation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea,rail or road.

Meanwhile, basically the Indonesian legal system currently accommodates the equivalent of the term e-commerce. The law that regulates the meaning of the term e-commerce is Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE). The ITE Law uses the term electronic transaction. The definition of Electronic Transaction is regulated in Article 1 point 2 which regulates as follows: "Electronic Transaction is a legal act conducted by using a computer, and / or other electronic media."

In practice, many people define electronic commerce differently. However, basically electronic commerce has basic characteristics, namely:

1. The availability of offers via the internet;
2. Transactions between 2 parties;
3. There is an exchange of goods, services or information
4. Using media that comes from the use of Information Technology. The internet is the main medium in this process or mechanism.

In Article 45 paragraph (2) of the Consumer Protection Law it is stated that:

"Settlement of consumer disputes can be pursued through the court or outside the court based on the voluntary choice of the disputing parties."

So in an effort to resolve consumer disputes according to the UUPK, there are two options for dispute resolution, namely:

1) Settlement outside the court, through an institution in charge of resolving disputes between consumers and business actors:

a. Amicable dispute resolution by the parties themselves
b. Settlement of disputes through an authorized institution, in this case the Consumer Dispute Resolution Agency by using the mechanism of conciliation, mediation, or arbitration.

2) Settlement of disputes through courts located within the general court.

Settlement of consumer disputes as referred to in Article 45 paragraph (2) of the Consumer Protection Law, does not preclude the possibility of peaceful settlement by the disputing parties, namely business actors and consumers, without going through a court or Consumer Dispute Resolution Agency, and as long as it does not conflict with UUPK. In fact, in the elucidation of the article it is stated that at each stage efforts are made to use a peaceful settlement by both parties to the dispute. From the explanation of Article 45 paragraph (2) of the Consumer Protection Law, it can be seen that the Consumer Protection Law requires that a peaceful settlement be a legal remedy that the disputing parties seek first, before the parties choose to settle their dispute through a consumer dispute settlement agency or judiciary.(manuhutu febrian leonardo, 2014)

In carrying out efforts to resolve consumer disputes outside the court, the Government forms a new agency, namely the Consumer Dispute Resolution Agency, for the settlement of consumer disputes outside the court. With the existence of the Consumer Dispute Resolution Agency, consumer dispute resolution can be done quickly, easily and cheaply, fast because the Consumer Protection Law stipulates that within a grace period of 21 working days the Consumer Dispute Resolution Agency is obliged to issue a decision.(Susanti Adi Nugroho, 2011). Easy because administrative procedures and decision-making processes are very simple. Cheap lies in affordable court fees. This is of course very useful in resolving e-commerce transaction disputes between businesses and consumers. Therefore, in the case of implementing e-commerce transactions between business actors and consumers, if a dispute occurs, it will be more appropriate to resolve it through out of court settlement, namely through the Consumer Dispute Resolution Agency (BPSK).

In the context of e-commerce dispute resolution, the role of BPSK is very important to immediately provide protection for traffickers. This is of course done in accordance with BPSK's duties, namely through the handling and settlement of consumer disputes by means of conciliation, mediation, or arbitration. Therefore, in order to carry out this task effectively in e-commerce dispute resolution, BPSK must also be able to adjust to the characteristics of the current electronic transaction and system administration. The operation of electronic systems and transactions is currently regulated in the ITE Law and PP PSTE. This means that BPSK should adjust to these provisions.

The difference between the operation of an electronic system for public services and the operation of an electronic system for non-publics can be found in several provisions in PP PSTE. In particular, administrators of electronic systems for public services are obliged to locate data centers and disaster recovery centers in the territory of Indonesia, must obtain an electronic system feasibility certification from the minister, and must be registered with the ministry that administers government affairs in the field of communication and information technology. In addition, the operation of electronic systems for public services is also required to use software registered with the ministry that administers government affairs in the field of communication and information technology, ensuring the safety and reliability of operations as appropriate, and in accordance with statutory provisions. If it is concluded, the implementation of an electronic system for public services demands to implement good and accountable governance. Basically, the same standard also applies to administrators of electronic systems for non-public services. However, the regulation is not rigidly regulated by opening up the possibility for non-public service providers to develop good and accountable governance.

4. Conclusion

1. The position of electronic signatures in electronic transactions in the prevailing laws and regulations confirms that electronic signatures can be used as evidence in court examinations. Electronic signatures

must meet the requirements according to legal provisions in Indonesia to be valid and meet the security aspects of electronic documents as stated in the ITE Law and PP PSTE. These aspects are authenticit, integrity, and non-repudiation. Legal recognition of electronic signatures in Indonesia through the provisions in the ITE Law, PP PSTE, POJK, and SEOJK shows that electronic signatures can replace the conventional signature function to show the agreement and competence of the parties according to the law, so that it can be used as evidence in the judge.

2. BPSK as the Operator of Electronic Transactions in the Scope of Public Services Based on the provisions of the Public Service Law and the ITE Law, BPSK can be categorized as a public service provider. Therefore, BPSK should adjust to the provisions regarding electronic system administrators within the scope of public services which are currently regulated under Government Regulation Number 82 of 2012 concerning Electronic System and Transaction Operation. If BPSK wants to provide protection for consumer dispute resolution in Indonesia, BPSK should have followed these provisions in order to carry out online dispute resolution (Online Dispute Resolution). Furthermore, as an electronic system operator within the scope of public services, BPSK needs to adjust to several provisions regarding the eligibility of electronic system administrators which include registration, hardware, software, experts, governance, security, and certification of electronic system eligibility.

References

Forder, J. dan D. S. (2008). Internet and E-Commerce Law.

Harahap, M. Y. (2004). Hukum acara perdata: tentang gugatan, persidangan, penyitaan, pembuktian, dan putusan pengadilan / M. Yahya Harahap. Sinar Grafika. http://lontar.ui.ac.id/detail?id=20161204

Hill, R. (1996). The Draft UNCITRAL Model Law for Electronic Commerce: Computer Lawyer (Frederick, Md.) 13:3:18-22, March 1996. https://unov.tind.io/record/6382

manuhutu febrian leonardo. (2014). Kedudukan Hukum Tanda Tangan Elektronik.

Susanti Adi Nugroho. (2011). Proses Penyelesaian Sengketa Konsumen ; di Tinjau dari Hukum Acara Serta Kendala Implementasinya /Susanti Adi Nugroho | Perpustakaan Universitas Terbuka. Kencana Prenada Media Group. https://opac.ut.ac.id/detail-opac?id=25417

Susanti Adi Nugroho. (2018). Proses Penyelesaian Sengketa Konsumen Ditinjau Dari Hukum Acara Serta Kendala Implementasiya.