Digital Signatures In the Minutes of Investigation By Investigators

Tri Janea Eka Putra[1], Riswadi[2]
{trijaneaekaputra@gmail.com[1], riswadi@borobudur.ac.id[2]}

Universitas Borobudur, Jakarta, Indonesia[1,2]

Abstract. Digital signatures on electronic documents can ensure the security of electronic information messages using public networks. A digital signature is a cryptographic mechanism implemented into an electronic signature and verified by the Electronic Certification Operator (PSrE). There seem to be differing viewpoints on the validity of electronic documents signed with digital signatures that are used as evidence in court. As per Law Number 11 of 2008 concerning Data and Digital Activities, which is further improved by Article 54 paragraph 1 of Regulation Number 82 of 2012, signatures have legal power and effects. If legalized by an electronic certification provider and subsequently demonstrated by a Digital Certificate, electronic signatures can be proof flawless complete such as a genuine deed.

Keywords: Signature; Digital; Certificate

1 Introduction

The condition of the whole world, which is currently still being hit by the COVID-19 pandemic, which has lasted from 2019 to the present, has made it difficult to hold meetings in person and has also had an impact on the current transportation system, which has begun to implement online siding as a solution to reduce face-to-face meetings and avoid the spread of Covid- 19, meanwhile from the side of law enforcement officers, in this case, investigators, there are still many cases of the spread of COVID-19 caused by meetings between investigators and people whose statements are taken as witnesses, experts or suspects.

Electronic or digital signatures can be a solution to the New Normal because it prioritizes the Low touch principle to minimize or even eliminate direct contact or touch between investigators and the person whose testimony is taken, either as a witness, expert, or suspect, even though there are obstacles in the application of digital signatures, one of which is uncertified and easy to imitate, Visually it is also difficult to distinguish between genuine or fake documents. In addition, the way we obtain certified electronic signatures or so-called digital signatures is what can be a protected solution through a statutory regulation in Law no. 11 of 2008. The dynamic pattern of Indonesian society appears to be continuing to move irregularly amid a desire to improve all aspects of life rather than a dependable thinking to establish a policy or proper structure. Despite the fact that the public has used a wide range of information technology products and telecommunications services in their daily lives, the Indonesian people as a whole are still groping for a public policy that will allow them to build

MIC 2021, October 30, Padang, Indonesia

DOI 10.4108/eai.30-10-2021.2315778

a reliable infrastructure (National Information Infrastructure) in the face of global information infrastructure [1].

Indonesia, which is in the era of globalization, is marked by the era of information technology which introduces cyberspace (cyberspace, virtual world) through the internet, communication with paperless electronic media. Through this electronic media, a person will enter the virtual world which is abstract, universal, independent of the circumstances of place and time [2]. Indonesian people believe that the role of information plays a role in contributing to economic, social, and cultural development. In addition, advances in information technology also affect social conditions in the future, such as the medical service system, education service system, government administration service system, and various other aspects of life [3]. An item or service using this information technology, from that information, if someone is interested in having a product or service offered, an electronic transaction will occur.

An equal position between legal protection, reliability, and security of information technology will create a "trust" to its users, without this trust electronic commerce and electronic government that is currently being promoted by the Indonesian government will not develop. This trust can be obtained by giving recognition laws against electronic writing. To this day, Indonesian law dictates that there is only one way to give legal force and legal consequences to a deed, namely by signing a manuscript. However, in trading practice, in particular, manuscript signatures have increasingly been displaced by the use of electronic signatures attached to dematerialized deeds or in other words "electronic deeds", so that there is a debate about recognition, legal force, and legal consequences of an electronic signature to its use. in a Minutes of Examination by the Investigator.

Electronic signatures are non-face (without meeting face to face), non-sign (not using an original signature), and without area boundaries (a person can electronically sign with other parties even though they are in different countries) using information technology. In its development, the security aspect of information has begun to be considered. When this information becomes damaged or there will be risks that must be borne by the people who send, need, or just view it, due to the use of this electronic information, using a public network, where everyone can find out the electronic information so that An independent and accountable institution that can verify the electronic signature and Indonesia has a legal rule to regulate this problem with the issuance of Law Number 11 of 2008, concerning "Electronic Information and Transactions" which was ratified on April 21, 2008.

So digital signatures as evidence in criminal evidence law are important because they involve the identity of the subject, the substance of the information, the fixation methodology, and the storage media that makes the information clear to know. How about the original signature as well as the information signed on paper converted to electronic data by scanner equipment, does it have legal force and legal consequences? Of course, it does not have legal force and legal consequences, because the signature is not made based on the agreed information or in other words the agreed information does not become the hand-making data, so that changes to the electronic signature and/or electronic information after the signing time cannot be is known.

Digital signatures appear in an electronic document that is not a written document (non-paperless). Based on this, the concept of digital signature is not following the legal principle which states that a document must be viewable, sent, and stored in paper form. Along with technological advances that continue to develop, considering that Indonesian law is more adaptable to Dutch law, where electronic signatures in that country have been recognized as having the same legal force as written signatures and have a high level of accuracy, it is

appropriate that the field of information and technology began to be accommodated into the procedural law system in Indonesia. This is important considering that electronic transactions are non-faced (without face to face) and non-signed (without a signature), causing many parties to doubt the power of proving digital signatures as evidence in court. Based on the background of the problem, the writer wants to research and compile a study entitled: "DIGITAL SIGNATURE IN THE MINUTE OF INVESTIGATION BY INVESTIGATORS".

2 Methodology

The research technique utilized in this work is normative juridical, and also the description of the data are secondary materials or data from the literature. which includes primary legal materials, secondary legal materials, and tertiary legal materials, with the primary legal materials being Law Number 11 of 2008 concerning Information and Electronic Transactions, Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions, and secondary legal materials being Law Number 11 of 2008 concerning Information and Electronic Transactions, secondary legal materials being Law Number 11 of 2008 concerning Information and Electronic as well as tertiary legal materials, namely Indonesian dictionary, legal dictionary,encyclopedias, and other legal materials.

3 Result and Discussion

The Covid-19 pandemic has caused various problems in life to date, including in the law enforcement sector, law enforcement officials, on the one hand, there is an obligation to complete case handling, on the other hand, the pandemic situation hinders the investigation and handling of cases, considering that examinations or court hearings will gather a lot of people so that it creates a vulnerability to the spread of Covid 19.

To this day, Indonesian positive law dictates that there is only one way to give legal force and legal consequences to a deed, namely by signing a manuscript. However, in trading practice, in particular, manuscript signatures have been increasingly displaced by the use of electronic signatures attached to dematerialized deeds. Electronic signatures and digital signatures are two things that often confuse their meaning and function, especially when signing documents. Although it doesn't look much different, in reality, A digital signature is not the same as an electronic signature. Electronic signatures cover a wide range of applications, while digital signatures are classified as one type of electronic signature.

Table 1. Comparison table of the difference between Electronic Signature and Digital Signature

Electronic Signature	Digital Signature
Used to verify documents	Used to secure documents
It can be in the form of images, writing, even a checklist	The form of a signature does not determine its validity
Do not have a document security system	Have a document security system
Cannot be validated	Can be validated by all individuals concerned with the document
Cannot guarantee document integrity	Document integrity can be guaranteed
Has no legal force	Has legal force
Does not have clear regulations	Registered and regulated under the authorities

From the description above we can see how electronic signature and digital signature are terms that are often used together but have significant differences. An electronic signature is not much different from a wet signature, only the physical form is different, one is in the form of electronic and the other is in the form of ink on paper. On the other hand, digital signatures have more complex and unique features that not only represent the individual but ensure authentication, integrity, and validity. Therefore, digital signatures are more widely used, especially because they have legal force. Both of these signatures have their respective functions depending on the needs of the user. Electronic Signatures and Digital Signatures are similar, but not the same. A digital signature is a signature made electronically that functions the same as a regular signature on a plain paper document [4].

Digital signatures can provide a guarantee of document security compared to ordinary signatures. Other proof for use besides electronic data or digital in the means of online signatures to be categorized by the recipient of an electronic message affixed with a digital signature could indeed verify whether the message came from the right sender and whether the message has been changed after being signed either intentionally or unintentionally in the case of electronic payments [5]. According to Article 18 of Law Number 11 of 2008, the strength of proof of an electronic document signed with a digital signature is the same as the strength of proof of an authentic deed made by an authorized public official, as explained in Government Regulation Number 82 of 2012 Article 52 paragraph 2 concerning the Operation of Electronic Systems and Transactions, which states that Electronic. Electronic Signatures are divided into two types based on Article 54 Paragraph 1 PP 82/2012, namely:

a. Certified Electronic Signature, which is evidenced by an Electronic Certificate and is created with the help of an electronic certification provider; and
b. Uncertified Electronic Signature, which is created without the help of an electronic certification provider and is not evidenced by an Electronic Certificate.

According to Article 54 above, what is meant by a certified electronic hand is what we call a digital signature. The digital signature has legal force as long as it meets the following requirements (a) Only the Signer has access to the Electronic Signature creation data; (b) Only the Signatories have access to the Electronic Signature creation data at the time of the electronic signing process; (c) Any changes to the Electronic Signature that occur after the signing time can be known; (d) All changes to the Electronic Information related to the Electronic Signature after the signing time can be known; (e) There are certain methods used to identify who the Signatories are. If we refer to the provisions of the law, then we can see how digital signatures by the Electronic System Operator must meet all the requirements of a certified electronic signature with legal force. Let's describe them one by one. The Electronic System Operator's digital signature ensures that points a and b are fulfilled by validating registration procedures with Dukcapil to liveness detection. The hash function mechanism for encryption and decryption ensures that points c and d are met. The requirements for points e and f are met by attaching a digital certificate to the document which can only be done by the owner of the digital certificate.

Meanwhile, the legal force of an uncertified electronic signature is the same as a wet signature as long as the electronic signature meets the requirements and complies with existing regulations. Electronic signatures or digital signatures have their respective roles and functions according to their abilities. You can use electronic signatures to identify documents or data on your behalf that do not require legal force or individual proof of validity, such as verification of receipt of goods delivered by logistics services, while for documents, activities, or processes directly related to an agreement or the validity of your data such as opening a credit

card, signing a contract, etc., should use a digital signature to make it more secure during the transaction process and minimize losses because it has legal force.

The use of digital signatures requires two processes, namely from the signatory and from the recipient. In detail the two processes can be explained as follows:

a. Formation of a digital signature using the hash value generated from the document as well as a predefined private key. To guarantee the security of the hash value, there should be a very small chance that the same digital signature can be generated from two documents with different private keys.
b. Digital signature authentication is the act of determining whether or not a digital signature was formed for the same document using the private key matching to the public key by referring to the original document and the public key that has been given. To sign a form or other piece of information, the signer must first choose which bits he or she wants to sign. The restricted information is called "message". The digital signature program will next use a private key to turn the hash value into a digital signature. Both the message and the private key have a unique digital signature as a consequence. In most cases, a digital signature is added to the document and preserved with it. A digital signature, on the other hand, can be transferred or kept apart from the document as long as it can be linked to it.

Since digital signatures are unique to the document, it is unnecessary to separate such digital signatures. The process of forming and verifying digital signatures fulfills the most important elements expected in a legal purpose, namely:

a. Signer Authentication: If the public key and private key pair are associated with a defined legal owner, the digital signature will be able to associate or associate the document with the signer. Digital signatures cannot be forged, unless the signer loses control of his private key.
b. Document Authentication: Digital signatures also identify signed documents with a much higher degree of certainty and accuracy than signatures on paper.
c. Assertion: Creating a digital signature requires the use of the private key of the signer. This action can confirm that the signatory agrees and is responsible for the content of the document.
d. Efficiency: The process of creating and verifying digital signatures provides a high level of assurance that the existing signature is a valid and genuine signature of the owner of the private key. With digital signatures, there is no need for verification by looking carefully (comparing) between the signature contained in the document with the original signature example as is usually done in manual signature checking.

Weaknesses that still accompany digital signature technology is:

a. Additional institutional costs: Digital signatures require the establishment of authorities entitled to issue certificates as well as other costs to maintain and develop their functions.
b. Subscription fee: The signer requires application software and also pays to obtain certification from the authority entitled to issue the certificate. While the most important advantage of having a digital signature is that the authentication of a document is more guaranteed. Digital signatures are very difficult to forge and are associated with a unique combination of documents and private keys.

Electronic Signature Process

To electronically sign a communication, the sender will first produce a message digest16 of the original message using the detachable typeface with the use of software (hash in English). Each original message's message digest is unique, like a "fingerprint," therefore even

the tiniest change in a message digest will result in a change in the "fingerprint." The advantage is that both the Sender and the Receiver may verify the message's integrity. The sender's private key will be used to sign the message digest, meaning that the electronic signature is a message digest encrypted with the sender's private key. The original comment and electronic signature are then forwarded to the intended recipient. The recipient may decode the electronic signature, say the result is A1, thanks to the Sender's public key, which is transmitted first to the message recipient. The receiver will then create a message digest on the original message received, say the result is A2. The final stage is to compare and contrast the two, namely A1 and A2. If both have the same "fingerprint," you know it's the original message that hasn't been tampered with.

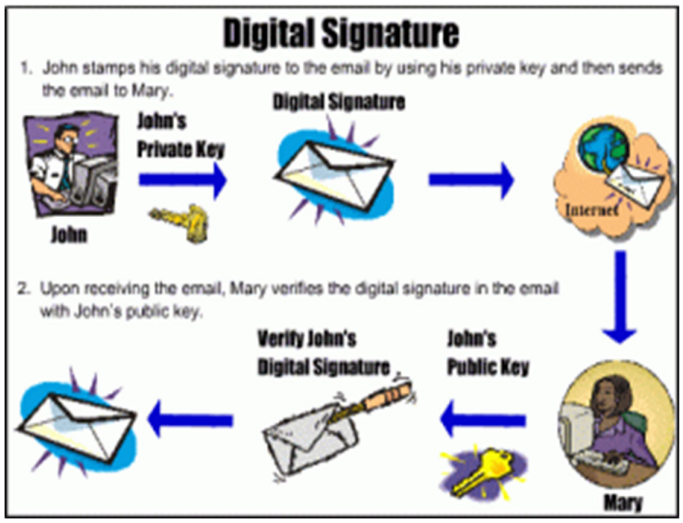

Fig. 1. Example of a digital signature' *tbibistel.wordpress.com,* 23 Mei 2011

The theory in this study uses the Legal Certainty Theory. Legal certainty is judicial protection against arbitrary actions, which means that a person will be able to obtain something that is expected under certain circumstances. The hope that the community wants with legal certainty is the main goal to be more orderly in social life. so that the law has the task of creating legal certainty which aims to produce public order. The theory of legal certainty contains two meanings [6]:

a. The availability of broad principles that enable people to comprehend what behaviors are permissible and which are not.
b. The existence of legal security in the form of assurances of legal certainty for individuals from government arbitrariness as a result of the existence of broad legal principles, allowing individuals to know what the State may do to them.

Legal certainty, according to Sudikno Mertukusumo, ensures that the legislation will be properly applied. Legal certainty necessitates efforts to control law through legislation enacted by authorized and authoritative persons, so that these regulations have a legal aspect that ensures legal certainty and may be used as a norm that must be followed. (7) Legal certainty may be viewed from two perspectives: certainty inside the law and certainty as a result of the law. In law, certainty means that any legal standard must be written in phrases that do not

allow for several interpretations. As a consequence, both compliant and disobedient behavior will be brought to the attention of the law. According to Article 75 paragraph (1) of Law Number 8 of 1981 concerning the Criminal Procedure Code ("KUHAP"), minutes are made for each action concerning (a) examination of suspects; (b) arrest; (c) detention; (d) search; (e) house income; (f) confiscation of objects; (g) mail inspection; (h) witness examination; (i) inspection at the scene; (j) implementation of court decisions and decisions; (k) carrying out other actions under the provisions of the law.

According to Article 75 paragraph (2), an official report is made by the official (investigator) concerned in carrying out the above actions and is made on the power of the oath of office. then based on Article 75 paragraph (3) the official report is not only signed by the official but also signed by all parties involved in the above actions. Article 10 paragraph (1) Number 14 of 2012, Regulation of the Head of the National Police of the Republic of Indonesia on the Management of Criminal Investigations ("Perkapolri 14/2012") Minutes of examination ("BAP") are included in the contents of the case file. And Article 15 letter d jo. Article 63 paragraph (1) Perkapolri 14/2012 Examination of witnesses is included in the realm of investigation.

According to the provisions of Article 1 point 2 of the Criminal Procedure Code, investigation is defined as a series of actions taken by investigators (police officers or civil servants with special authority to investigate) in accordance with and according to the method set forth in the Criminal Procedure Code to seek and collect evidence in order to clear the perpetrator of the crime and locate the suspect. Investigation activities based on Article 15 of Perkapolri 14/2012 are carried out in stages including: (a) investigation; (b) SPDP delivery; (c) coercive effort; (d) inspection; (e) case title; (f) settlement of case files; (g) submission of case files to the public prosecutor; (h) surrender of the suspect and evidence; and (i) cessation of the investigation.

Article 63 paragraph (1) and paragraph (2) of Perkapolri 14/2012 states that the examination is carried out by investigators/assistant investigators against witnesses, experts, and suspects, To make the case obvious, acquire testimony from witnesses, experts, and suspects as described in the BAP. so that the role of a person and evidence in a criminal incident may be clearly understood The investigator/assistant investigator conducting the examination and the individual being examined must both sign the examination as specified in this BAP. The preparation of the BAP related to the examination of witnesses by investigators in outline is as follows:

a. Yahya Harahap in the book Discussion of Problems and the Application of the Criminal Procedure Code: Investigation and Prosecution (8) describe the statements presented by witnesses in the investigation, carefully recorded by investigators in the BAP. The principle of recording witness testimony is that it is recorded according to the words used by the witness.
b. Yahya Harahap (p. 143) further explained that the official report containing witness statements was signed by both the investigator and the witness. In signing the minutes of examination, two things must be considered:
    1. The witness signed the BAP after having first approved the contents of the report. [Article 118 paragraph (1) KUHAP]. Was this approval given after the investigator read it before him or did the investigator order him to read it himself? Yahya Harahap explained that the second method is actually the best, if the witness is good at reading. But if he cannot read, there is no other choice but to read the minutes in front of the witness by the investigator.

2. The law provides the possibility for witnesses not to sign the BAP. [Article 118 paragraph (2) of the Criminal Procedure Code]. If the witness does not want to put his signature in the BAP, the investigator makes a note of this refusal in the official report. The note is in the form of an explanation of the reasons why the witness refused to sign in the official report. If the witness does not want to sign the official report, he must give a strong reason [explanation of Article 118 paragraph (2) of the Criminal Procedure Code].

c. For witnesses who are suspected of having sufficient reasons to be unable to attend the trial in court, an oath or promise may be made before the examination is carried out and an official report is made. [Article 64 paragraph (2) Perkapolri 14/2012]

At the level of legal practice, especially in the judicial environment, a process of digitizing evidence has been carried out from the digitization process in the judiciary, the best known is Virtual civil courts, in Indonesia, we know it as an integrated unit in the e-court system. The maximum benefit has been running since the issuance of Supreme Court Regulation (Perma) Number 1 of 2019 concerning administration and trial in court electronically. The system has now become a solution for court institutions under the Supreme Court (MA) to continue to provide legal services even though justice seekers are not present in court. The use of e-courts ultimately leads to the importance of implementing virtual courts that are held online without the need to present the parties in the courtroom,

Then, observing these developments, the Prosecutor's Office carried out the initiation through the Attorney General's Instruction Number 5 of 2020 dated March 23, 2020, which encouraged a breakthrough in holding trials during the Covid 19 pandemic online through Video Conference facilities, of course, this was also in collaboration and coordinated with the Supreme Court (MA), The Indonesian National Police (Polri) and the Penitentiary (LP) as interested institutions, then the Indonesian Attorney General's Office, Through agreement Number: 402/DJU /MH.01.1/4/2020, Number KEP-17/E/Ejp/04/2020, Number PAS-08.HH.0505 about the trial via teleconference on April 13, 2020, the Supreme Court and the Ministry of Law and Human Rights entered into a cooperation agreement pertaining to online trials. The application of video conferences in examining cases in trials in Indonesia, especially criminal cases, is not new, before the COVID-19 pandemic, video conferencing technology had been used in several cases, especially to hear statements from witnesses.

This is regulated in Article 9 paragraph (3) of Law Number 31 of 2014 concerning amendments to Law Number 13 of 2006 concerning the protection of witnesses and victims, where a witness can hear his testimony directly through electronic means accompanied by an authorized official. This conference aims to protect the security of witnesses from various threats or to facilitate the provision of information without having to be present in the courtroom. Based on the above, the use of video conferences in examining witnesses by investigators can also be carried out, and after that to respond to the implementation of social/physical distancing (social/physical restrictions) and even lockdown (regional quarantine) then it needs to apply the minutes of examination by investigators using digital signatures.

4 Conclusion

Digital signatures appear in an electronic document which is basically not a written document (nonpaperless). As a result, the electronic signature and digital signature concepts violate the legal premise that a document must be visible, transferred, and preserved in paper

form. Along with technological advances that continue to develop, considering that Indonesian law is more adaptable to Dutch law, where electronic signatures in that country have been recognized as having the same legal force as written signatures and have a high level of accuracy due to certification by the Certificate Authority. or in Indonesia the Electronic Certification Operator (PSRE) then it is appropriate if the information and technology sector begins to be accommodated into the procedural law system in Indonesia. This is important considering that electronic transactions are non-faced (without face to face) and non-signed (without a signature), causing many parties to doubt the power of proving electronic signatures as evidence in court.

According to the preceding statement, digital signatures can be employed as legal evidence and have the same full and perfect proof capacity as an original deed. It should be noted that when an examination of a civil case in court presents an electronic signature as evidence, then following the legal principle of lex derogate lex generalis above, prosecutors and judges must be guided by the provisions stipulated in Law no. 11 of 2008 concerning Information and Technology, although the Criminal Procedure Code does not regulate digital signatures as legal evidence. The use of digital signatures in the minutes of examination by investigators as evidence at the trial is a solution to current and future conditions.

References

[1] Maria Farida Indrati Soepapto, Ilmu perundang-Undangan, Dasar-Dasar dan Pembentukan, Kanisius, Jakarta, (1998)

[2] Mariam Darus Badrulzaman, Mendambakan Kelahiran Hukum Saiber (Cyber Law) di Indonesia, Pidato Purna Bhakti, Medan, 13 Nopember 2001.

[3] Ibid.

[4] Ahmad Suwandi, B.Setyo Ryanto, Menabur Sentuh, Menuai, Software Tangguh, PC Media (2004).

[5] Abdul Halim Barkatullah, Teguh Prasetyo, Bisnis E-Commerce, Yogyakarta, Pustaka pelajar (2005)

[6] Peter Mahmud Marzuki, Pengantar Ilmu Hukum, Kencana Perdana Media Group, Jakarta (2008)

[7] Asikin Zainal, Pengantar Tata Hukum Indonesia, Rajawali Pers, Jakarta (2012)

[8] Harahap, Yahya. Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan. Jakarta: Sinar Grafika (2008)