EXAMINING THE LEGAL STANDING OF DIGITAL SIGNATURES UNDER CIVIL AND ITE LAWS

Desak Ayu Intan Diah Iswari[1*], Dewa Gede Rudy[2]
[1,2] Faculty of Law, Universitas Udayana
E-mail: [1)] iiintandiahh@gmail.com

Abstract

This research aims to investigate the validity of digital signatures and their evidential value. This study adopts a normative juridical approach, utilizing a statutory method. The findings of this study reveal that: (1) Digital signatures have evidential strength as they are recognized by Article 5 of the ITE Law and are legally binding in civil cases in accordance with the relevant procedural laws of Indonesia. (2) In terms of legality under Indonesian positive law, digital signatures contained in electronic documents are considered valid in civil law, in accordance with the provisions of Article 1320 of the Civil Code and the enactment of Law Number 19 of 2016 Amendment to Law Number 11 of 2008, as well as Government Regulation No.71 of 2019, which deals with the Implementation of Electronic Systems and Transactions.

Keywords: *Digital Signatures, Evidential Value, Validity, ITE Law, Electronic Documents*

1. INTRODUCTION

The COVID-19 pandemic has been making headlines across various countries for the past three years, causing significant changes in people's lifestyles and prompting social, economic, cultural, defense, security, and law enforcement changes (WHO, 2020). Alongside the pandemic, terms such as "new normal," "virtual meetings," and "Zoom meetings" have become commonplace (Kukah et al., 2022). The influence of globalization and the use of information and communication technology have further led to changes, resulting in a new way of life. However, these changes have also brought about negative impacts, such as the rise of unlawful acts in cyberspace (Baz et al., 2021). Therefore, to ensure legal certainty, the government has an obligation to regulate the utilization of information and communication technology.

The emergence of various new phenomena resulting from advances in technology and information has had a significant impact on the lives of global communities, particularly the development of information technology. The era of information technology introduces cyberspace, which is characterized by an interconnected network (internet) that employs paperless communication (Babbar & Chandhok, 2008). Electronic transactions are non-face-to-face, do not require wet signatures, and are borderless, allowing individuals to conduct them with others in different countries using information technology.

With the increasing development of information technology, security aspects have become a growing concern (Ikenwe et al., 2016; White, 2016). When information is advanced, there are risks that must be considered by individuals, including those who send, receive, or view it. This is because the use of electronic information involves a public network, making electronic information accessible to everyone. In cases where one party fails to fulfill the agreed-upon terms of an electronic transaction with the other party, this can be detrimental to those who use information technology for the sale of goods or services.

Legal issues related to the electronic delivery of information, communication, and transactions often arise, especially in terms of evidence and legal actions taken through electronic systems (Manggala et al., 2021). These issues are particularly pressing in the civil sector, as electronic transactions in e-commerce have become an integral part of national and international trade. The convergence of information technology, media, and informatics continues to develop rapidly, in line with new advances in these fields (Harwanto, 2022).

To address these issues, the Indonesian government enacted Law No. 11 of 2008, which was later amended to Law No. 19 of 2016 on Electronic Transactions and Information (hereafter referred to as the ITE Law). One of the critical aspects to consider in electronic transactions is the implementation of a digital signature, which aims to legalize documents or results in electronic transactions. The ITE Law No.19 of 2016 regulates the authentication of rights and obligations in an electronic document that is digitally signed (digital signature).

In today's world, where incidents of data tampering and forgery are becoming increasingly prevalent, it is essential to protect any data sent online (Masur, 2020; Monteleone, 2015). For this reason, digital signatures are gaining popularity among professionals due to their ability to validate the authenticity of a document, file, or software. However, Indonesian positive law only recognizes manuscript signature as the legal force and consequence of a document, despite the increasing displacement of manuscript signatures in trade practices with the use of electronic signatures attached to a document or commonly referred to as electronic documents. This has resulted in debates about the recognition, legal force, and legal consequences of an electronic signature or digital signature, particularly in the context of commercial transactions.

Despite this, trade practices have increasingly displaced manuscript signatures with the use of electronic signatures attached to a document or commonly referred to as electronic documents. This has resulted in debates about the recognition, legal force, and legal consequences of an electronic signature or digital signature, particularly in the context of commercial transactions (Hudzaifah, 2015).

In e-commerce activities, electronic documents with digital signatures can be categorized as written evidence (Mayasari, 2022). However, there is a legal principle that makes it difficult to develop the use of electronic documents with digital signatures, which is the requirement that the document must be visible and stored in paper form. Problems arise when someone wants to make a transaction, such as the purchase of goods. The parties are then faced with various legal issues, including the validity of the documents, digital signatures, the binding force of the contract, and the cancellation of the transaction. One possible solution to this issue is the use of electronic signature laws that have been enacted in many countries. These laws provide a legal framework for the use of electronic signatures and documents, making them equivalent to their paper counterparts.

For example, in the United States, the Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA) provide legal recognition for electronic signatures and documents in interstate and intrastate transactions, respectively (Wittie & Winn, 2000). These laws ensure that electronic documents and signatures are legally enforceable and have the same legal effect as their paper counterparts.

Similarly, in the European Union, the eIDAS regulation was enacted in 2016 to provide a common legal framework for electronic identification and trust services (Dumortier, 2022). It establishes the legal validity of electronic signatures and ensures their cross-border recognition throughout the EU.

As for Indonesia, so far we have known various digital signatures / types of signatures, namely those in the form of wet thumbprint signatures, electronic signatures, and signatures made by scanning processes such as signs in general or conventional signatures, signatures in their use are recognized in evidentiary law which still need specific study are related to digital signatures / digital signatures.

The validity of electronic signatures/digital signatures in an agreement from the perspective of civil law in Indonesia refers to the ITE Law No. 11 of 2008, which amends Law No. 19 of 2016 on Electronic Information and Transactions, and Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions as implementing regulations for electronic transactions. These are then associated with the Articles of Evidence and the principles of agreement in the Civil Code, where if one of the parties defaults or breaches the promise, legal steps can be taken.

Furthermore, electronic signatures appear in an electronic document that is essentially not a written document (non-paperless). Based on this, the concept of electronic signatures is not in accordance with legal principles that state that a document must be visible, sent, and stored in paper form. With the advancement of technology, it is appropriate that information and technology be accommodated into the civil law system in Indonesia. Hence, many parties doubt the validity of the current digital signature/digital signature both in the scope of the trial and in the agreement process.

Overall, the use of electronic signatures and documents can provide numerous benefits in terms of efficiency, cost savings, and convenience in e-commerce transactions. However, the legal framework for their use must be established to ensure their validity and enforceability. As such, it is important for businesses to familiarize themselves with the applicable laws and regulations to ensure compliance and mitigate legal risks.

This study aims to explore the legal principles that govern the use of electronic documents with digital signatures in e-commerce activities. The findings of this research will have significant implications for the legal framework governing e-commerce transactions, which will facilitate the development of digital technologies in the business environment. Additionally, the results of this study will provide insights into the practical implications of using electronic documents with digital signatures, which will be useful for legal practitioners, policymakers, and business owners.

2. RESEARCH METHODS

This study utilized the normative juridical research method, which involved analyzing library materials such as literature, laws, and regulations, as well as agreements related to the research problem (Soekanto, 2007). The research approach consisted of two parts: a statute approach and a case approach. The statute approach involved examining all relevant laws and regulations related to the legal issues being studied, while the case approach focused on analyzing relevant court cases and other legal precedents. By combining these two approaches, this study aimed to provide a comprehensive understanding of the legal issues at hand.

3. RESULTS AND DISCUSSION

3.1. The Evidentiary Value of Digital Signatures in the Legal System

1) Civil Case Proof in Indonesia

Evidence is the presentation of valid evidence according to the law by litigants to the judge in a trial with the aim of bolstering the truth of legal arguments concerning the facts in dispute. Evidence plays a central role in the judicial process, particularly in civil cases, where parties have the opportunity to demonstrate the veracity of the legal facts at issue during the evidentiary stage.

In Indonesia, positive evidentiary law is still based on the HIR / RBg and BW Book IV, which were products of the Dutch East Indies government (Kusmayanti & Anrova, 2021). The evidentiary law contained in the HIR and RBg is formal evidentiary law, while in BW, it is material evidentiary law. Material evidentiary law regulates the admissibility of certain evidence in court and its evidentiary power, while formal evidentiary law regulates how to conduct proof.

Evidence is a crucial element of court proceedings that helps judges to apply the law and make decisions. The Civil Code specifies the types of valid evidence and their respective evidentiary powers in Article 1866. Article 164 of the HIR / 284 of the RBg and Article 1866 of the Civil Code define the evidence that can be used to settle civil disputes in a limitative manner, arranged in sequence from letter evidence, witness testimony, suspicions, confessions, and oaths.

In the Civil Code, evidence is generally regulated in Book Four (IV), which covers Evidence and Expiration. The civil procedural law follows the principle of "Seeking Formal Truth" regarding the evidentiary system, meaning that the judge is passive when examining the case. Therefore, the judge is not allowed to take active initiatives in adding or submitting necessary evidence because it is the right of each party to do so.

One of the judge's responsibilities in seeking formal truth is to investigate whether the legal relationship that forms the basis of the lawsuit actually exists or not. The plaintiff must prove the existence of this legal relationship to win the case. Another principle of civil case evidence is that decisions must be based on proven facts presented during the trial. Judges cannot make decisions without evidence. The rejection or granting of a lawsuit must rely on evidence derived from facts submitted by the parties. Proof can only be enforced based on the support of facts; proof cannot be enforced without existing facts.

With the advancements in information technology and telecommunications, new forms of evidence in civil relations have emerged. These developments in society have led to the emergence of various types of modern transactions, which have given rise to evidence that is not regulated by the rules of civil procedure (HIR / RBg). From photocopies to electronic evidence, society's progress is accompanied by advancements in information technology and telecommunications, leading to new types of evidence in civil legal relations.

According to literature, photographs (portraits) and sound or image recordings, including CCTV recordings, cannot be used as evidence because they can be fabricated and do not necessarily prove what actually happened. However, with technological advancements in the field of information and telecommunications, the originality of a photograph and sound or image recording can now be determined using specific techniques.

Although the law of evidence has regulated valid evidence in detail, in some civil disputes, particularly those related to e-commerce, electronic signatures/digital signatures are used as evidence in court. However, evidence in such cases is limited to what is specified in Article 1866 of the Civil Code. The presence of ITE Law No.19 of 2016 and PP No.71 of 2019 provides further legal support for the use of digital signatures/electronic signatures attached to an electronic document.

2) Digital Signature Evidence at Trial

The emergence of Industry 4.0 has led to many physical activities being replaced by digital-based industries. To improve time and cost efficiency, the concept of digital signature, also known as electronic signature, has become a popular way of signing contracts.

Digital signature can be used to verify the authenticity and validity of electronic evidence, such as documents or electronic information (Hudzaifah, 2015). Unlike a handwritten signature that is physically attached to a document, a digital signature consists of two cryptographic keys, a public key and a private key, that authenticate each other. The person creating the digital signature uses their private key to encrypt the data associated with the signature, while the only way to decrypt the data is with the signer's public key.

The purpose of a digital signature is to ensure the authenticity of the document by marking it in a way that identifies the sender and ensures that the integrity of the document is not changed during transmission. This is done through the use of hash functions, which produce a unique value for each data entered. If there is a change in the document content, the hash value generated will be different, allowing the recipient to compare the hash value. If the hash value is the same and appropriate, then the data is authentic, and its authenticity is guaranteed. Conversely, if the hash value is different, then the data is suspicious and has likely been modified.

The use of digital signature in the process of forming an agreement or contract (e-commerce) facilitates the proof mechanism in civil cases by showing where the electronic data came from and guaranteeing the integrity of the message. This can be done through the existence of a digital certificate obtained from a certification authority by the user or subscriber.

The process of proving only occurs if there is a dispute between the parties, which is usually resolved by a clause in the agreement. Generally, settlement is through litigation or non-litigation. Evidence is one of the most important things in the process of resolving civil disputes in court. The evidentiary stage is used to prove the existence of an event and whether one of the parties was involved or not in front of the trial. With the existence of evidence, the parties try to establish the truth of an event, or by using evidence to prove whether the party actually carried out the event or not. This allows the judge to obtain the necessary information to make a decision and resolve the dispute in the trial.

The recognition of a digital signature as valid evidence can be seen from the provisions of Law No.19 of 2016 concerning Electronic Information and Transactions, and Law No.11 of 2008 concerning ITE. Article 5 of the law states that "Electronic information and/or electronic documents and/or their printouts are valid legal evidence and are an extension of valid evidence in accordance with the applicable Law of Procedure in Indonesia in accordance with the provisions regulated in this Law."

Based on the above provisions, it is explained that electronic signatures can be used as valid evidence in court, similar to other evidence regulated in the Civil Code. Therefore, Article 1869 jo Psal 1874 of the Civil Code and Article 1 of Ordinance 1867 No.29 apply, ensuring that the electronic/digital signature attached to the electronic document has legal force. The act of signing confirms agreement to the information or electronic document signed and guarantees the accuracy of the contents in the writing.

With the issuance of Law No.11 of 2008 concerning Electronic Information and Transactions jo Law No.19 of 2016, there was a development in the law of evidence. Previously, electronic evidence could only be used as presumptive evidence in civil cases or as evidence of clues in criminal cases. However, electronic documents and printouts are now firmly recognized as valid evidence in court, as long as they meet certain conditions as determined by law. Article 6 states that electronic information and electronic documents can be used as evidence in court. Nevertheless, each electronic information/document is considered valid evidence only if it is accessible, displayed, guaranteed integrity, and accountable.

For electronic documents or electronic information to be considered valuable evidence, they must be able to explain a situation. In a trial, a key issue is the comparison of wet signatures in a traditional deed or letter with electronic/digital signatures in an agreement (such as e-commerce transactions). Article 11 paragraph (1) of Law Number 19 of 2019 concerning amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions confirms that electronic/digital signatures have legal force and legal consequences.

Various mechanisms can be used for producing electronic signatures, as mentioned in Article 59 of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. However, not all electronic signatures carry legal force and legal consequences.

The provisions of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning ITE explain that electronic/digital signatures have legal force and can be used as valid evidence in court as long as they meet the applicable requirements. Further provisions can be found in Article 11 of the ITE Law, which states that "Digital Signature/Electronic Signature has legal force and legal consequences as long as it meets the following requirements: (a) the data for making electronic signatures is related only to the signatory; (b) the data for making electronic signatures during the electronic signing process is only in the power of the signatory; (c) any changes to electronic signatures that occur after the time of signing can be known; (d) any changes to electronic information related to the electronic signature after the time of signing can be known; (e) there are certain ways used to identify who the signatory can be known; (f) there are certain ways to show that the signatory has given approval to the related electronic information."

Compared to wet signatures that can be copied and require laboratory examination to prove identical or non-identical signatures, the security of electronic signatures is ensured by asymmetric cryptography. Each bit of a digital signature is encrypted by a legitimate issuing institution, certifying the authenticity and security of the electronic signature through a hardware security module (HSM). The combination of hardware, software, and procedures provides additional protection against unauthorized access.

The above description highlights the importance of electronic documents signed with digital signatures, particularly after the issuance of Law No.19 of 2016 concerning

Electronic Information and Transactions and Government Regulation No.71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Recognition of electronic documents signed with digital signatures is an extension of the proof of civil procedural law in Indonesia, such that all electronic transactions with electronic signatures are considered as deeds with the same evidentiary strength as traditional deeds, provided that the digital signature is a certified electronic signature issued by an Electronic Certificate Operator (PSrE) licensed by the Ministry of Communication and Information.

The validity of a digital signature/electronic signature depends on whether it is certified or uncertified. If a party disputes the validity of an electronic signature, the judge must obtain expert testimony from the digital certificate issuing institution to determine whether the signature is valid and issued by the institution. In the case of an uncertified electronic signature, its validity is similar to that of a disputed wet signature, which must be resolved through laboratory examination. These provisions highlight the importance of electronic signatures in modern business and legal transactions, and the need for robust security measures to ensure their reliability and authenticity.

3.2. The Validity of Digital Signature Viewed from The Perspective of Civil Law and ITE Law

1) Regulation on Digital Signatures in Indonesia

Digital signatures/electronic signatures are gaining popularity in Indonesia as they offer a convenient and efficient way to sign contracts without face-to-face interaction or physical documents. Despite its many benefits, there are doubts about whether digital signatures can be legally recognized in Indonesia. Signatures are a fundamental part of society and are important for representing agreement on a matter. They serve four main purposes, including providing evidence, indicating approval, fulfilling formalities, and improving efficiency. Therefore, it is crucial to have a law that regulates digital signatures/electronic signatures.

In his book, Tan Thong Kie explains that a signature serves as a statement of the signer's will, indicating that they intend for the written text to be considered their own by affixing their signature underneath it (Kie, 2000). This concept is also reflected in Article 1875 of the Civil Code, which states that a written document bearing a signature recognized by the person to whom it is presented or deemed to be justified by them, carries the same weight as an authentic deed for the signatory, their heirs, and those who receive rights from them.

Thus, according to the Civil Code, the validity of a signature depends on the recognition of the signer. As a new technology innovation in Indonesia, digital signatures / electronic signatures are now regulated by legislation, including the 2008 Law on Electronic Information and Transactions (ITE) and its 2016 amendment, Law No. 19 of 2016 on Electronic Information and Transactions, which specifically address the use of digital signatures / electronic signatures and electronic certificates.

Since the enactment of the ITE Law in 2008 and its amendment to Law No.19 of 2016, it has been the foundation for the implementation of digital signature technology / electronic signatures in Indonesia. However, it was only in 2012 that a government regulation was issued, which was later amended to PP No. 71 of 2019 concerning the Implementation of electronic systems and transactions, that became the legal basis for

online transactions and the implementation of digital signatures / electronic signatures in Indonesia.

Based on existing laws and government regulations, digital signatures / electronic signatures must have supporting technological capabilities that ensure the fulfillment of predetermined requirements. These requirements include the attributes of a digital signature / electronic signature and its ability to verify.

Regarding the attributes of digital signature / electronic signature, authentication capability is crucial to guarantee the authenticity of digital signatures / electronic signatures and digital documents. This is because digital technology allows anyone to copy and duplicate documents and digital signatures / electronic signatures themselves. Therefore, the authentication aspect of digital signature/electronic signature is essential.

Digital signatures / electronic signatures have two aspects that need to be fulfilled for their validity:

1. Authentication of the owner of the digital signature / electronic signature. This means that the electronic signature must be owned by the person who signed the digital document.
2. Document authentication. Digital documents must be authenticated after being signed to ensure that they remain unchanged and cannot be falsified.

Therefore, with the enactment of Law No. 19 of 2016 amending Law No. 11 of 2008 on Electronic Information and Transactions, and Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, digital signatures / electronic signatures have legal recognition in Indonesia.

Law No.71 of 2019 concerning the Implementation of Electronic Systems and Transactions, Article 60 paragraph (2) identifies at least two types of digital signatures / electronic signatures: (a) certified electronic signatures, which must meet the requirements for validity, legal force, and legal consequences of electronic signatures as referred to in Article 59 paragraph (3). This type of electronic signature must use electronic certificates issued by an Indonesian Electronic Certificate Service provider and be created using a certified electronic signature-making device. (b) Uncertified electronic signatures, which are made without using an electronic certificate service provider.

PP No. 80 of 2019 concerning Trade through Electronic Systems further regulates that "proof of transactions using certified or indented electronic signatures can be considered as authentic written evidence" in Article 49 paragraph 3. Certified electronic signatures must be provided by an Indonesian Electronic Certificate Provider (PSrE Indonesia) that has passed an audit referring to the standards issued by the Ministry of Communication and Information Technology (Kominfo) under Article 1 number 5 of Permenkominfo No.11/2018 concerning the Implementation of Electronic Certification. An electronic certificate organizer is defined as a legal entity that functions as a trusted party providing and auditing electronic certificates.

A certified digital signature / electronic signature is made using an electronic certificate issued by PSrE Indonesia (Haryanto et al., 2020). According to the ITE Law, an electronic certificate is a file that contains digital signatures / electronic signatures and identities that indicate the legal status of the parties involved in electronic transactions, and is issued by PSrE Indonesia. In short, electronic certificates are files that can prove a person's identity and validate electronic signatures, ensuring the authenticity, integrity, and non-repudiation of information signed with electronic signatures.

Certified digital signatures / electronic signatures that use electronic certificates provide three guarantees of trust for the owner. Firstly, they guarantee data authenticity by showing the identity of the certificate owner in electronic documents. Secondly, they ensure integrity so that activities in electronic documents that have been signed can be monitored. Finally, they guarantee non-repudiation, proving the authenticity of the signature so that the signer cannot deny having made electronic transactions.

Certified and uncertified digital signatures/electronic signatures differ fundamentally in terms of data validity and legal certainty. The validity and legal certainty can only be provided by an electronic certificate provider (PSrE) licensed by the Ministry of Communication and Information (KOMINFO). There are currently at least nine recognized electronic certification providers in Indonesia, including Privy Digital Identity (PrivyID), Indonesia Digital Identity (VIDA), Djelas Signature Bersama, Tilaka Nusa Teknologi, Digital Signature Asli, Printing Money of the Republic of Indonesia (PERURI), Solusi Net Internusa (Solusi Net), National Research and Innovation Agency (BRIN), and Electronic Certification Center of the State Cyber and Crypto Agency.

According to the ITE Law, a certified Digital Signature/Electronic Signature is considered valid in the eyes of the law when it meets several requirements. Firstly, the electronic signature creation data should be related only to the signer. Secondly, the electronic signature creation data should only be in the power of the signatory during the electronic signing process. Thirdly, any changes to electronic signatures that occur after the time of signing should be known. Fourthly, any changes to electronic information related to the electronic signature after the time of signing should also be known. Fifthly, a certain method should be used to identify the signer. And sixthly, there should be a certain way to show that the signing has given approval to the related electronic information.

Verification capability is the next step in digital signature/electronic signature verification. Verification is needed to prove that the electronic signature included in the digital document is indeed an authentic signature. This verification capability is crucial to ensure that digital signatures are not forged or used by parties other than the signature owner.

2) Mechanism Attributes of Digital Signature/Electronic Signature Procedure

A digital signature or electronic signature requires proof of identity to ensure that the correct person is signing the document (Khrykova et al., 2021). This is accomplished using a cryptographic algorithm known as a hash function, which creates a unique electronic signature. The hash allows for the storage of personal data such as biometric records without the risk of it being copied by unauthorized parties. To access this information, a token device or an identity verification system, such as a biometric scanner, is required to authorize a person to sign.

All technological capabilities for electronic signatures must be provided by the Electronic Certificate Provider or PSrE. The PSrE must receive certification from the regulator, which in this case is the Ministry of Communication and Information, to issue electronic certificates for certified digital signatures or electronic signatures.

Regarding the procedure for creating a digital signature or electronic signature, the applicant must register through the Indonesian service (PSrE) that has received recognition from the Ministry of Communication and Information to issue electronic certificates. Electronic certificates are electronic certificates in electronic form that

contain electronic signatures and the identity of the legal subjects of the parties involved in electronic transactions, issued by PSrE Indonesia.

As previously mentioned, the digital signature / electronic signature and identity of the legal subject of the parties in electronic transactions are issued by PSrE Indonesia. Additionally, the Ministry of Communication and Information has described three stages that must be completed by the applicant to obtain an electronic certificate for a certified digital signature / electronic signature.

1. Submission Stage: The applicant registers with PSrE Indonesia and must meet the specific requirements of each PSrE Indonesia, which can be found on their respective websites. Applicants who work as State Civil Apparatus (ASN) must register with the Government PSrE.
2. Verification Stage: PSrE Indonesia verifies the applicant's data and compares their population data, such as NIK, name, date of birth, photo, and biometric data (fingerprints), to the authorized population data management database of the Ministry. If the data is valid and correct, the issuance process will continue.
3. Issuance Stage: Applicants who have passed the verification stage will be provided with an account to download the electronic certificate issued by PSrE Indonesia. This account can also be used to manage digital signature/certified electronic signature services, certified electronic seals, and other services that can be used as a substitute for company seals. Once the owner has an electronic certificate, they can sign electronic documents anytime and anywhere using various platforms such as global digital business, e-banking, peer-to-peer lending services, agreements, and more.

Security features used in digital signatures/electronic signatures to ensure that documents are not altered and that digital signatures/electronic signatures are valid include:

1. PINs, passwords, and codes: Used to authenticate and verify the identity of the signer and approve their signature. Email, username, and password are common examples.
2. Time stamping: Provides the date and time of the signature, which is useful for legal proceedings and situations where time is critical, such as stock trading or lottery ticket issuance.
3. Asymmetric cryptography: Uses a public key algorithm that includes both private and public key encryption/authentication.
4. Checksum: A long string of letters and numbers representing the correct digits in a piece of digital data, which can be used for comparison to detect errors or changes. The checksum acts as a fingerprint of the data.
5. Cyclic redundancy checking (CRC): An error detection code and verification feature used in digital networks and storage devices to detect changes to raw data.
6. Certificate Authority (CA) validation: CAs issue electronic signatures and act as trusted third parties by accepting, authenticating, issuing, and maintaining digital certificates. The use of CAs helps avoid the creation of fake digital certificates.

7. Trust Service Provider (TSP) validation: A TSP is a person or legal entity that performs digital signature validation on behalf of a company and offers signature validation reports.

Starting from the description above, the presence of a digital signature/electronic signature begins with an agreement between two parties who then enter into a contract. Therefore, we refer to Article 1320 of the Civil Code, which states the legal requirements of an agreement, including:

1. There is an agreement for those who bind themselves;
2. The readiness of the parties to make an agreement;
3. A certain thing;
4. A halal cause (causa).

The agreement must be based on the consensus or agreement of the parties. With the principle of consensualism, the agreement is said to have been made if there is an agreement or conformity of will between the parties. No agreement, no contract (no consent no contract).

In an agreement that uses digital signatures, the agreement is considered valid since the agreement has been reached. In Article 1338 paragraph (1) of the Civil Code, it is stated that "all legally made agreements shall be binding for those who make them." From the wording of this provision, the agreement is binding if it fulfills the conditions for the validity of the agreement.

The consensual principle states that an agreement is born once the agreement is reached, and to reach an agreement, there must be a statement of will. Therefore, as long as the parties to the digital signature / electronic signature recognize the agreement, it is valid. However, if one party denies it, that party must prove it.

Based on Article 1338 paragraph (1) of the Civil Code, "All agreements made legally shall apply as laws for those who make them." Therefore, an agreement that includes a digital signature / electronic signature remains binding as long as there is no denial from the party making the agreement. To assess the validity of an agreement with a digital signature / electronic signature, it is necessary to analyze its validity based on the provisions of Article 1320 and Article 1338 of the Civil Code, Law No.11 of 2008 jo Law No.19 of 2016 concerning Electronic Information and Transactions, and PP NO.71 of 2019 concerning System Administration and Electronic Transactions.

4. CONCLUSION

In conclusion, the digital signature has become a crucial addition to the positive civil law system in Indonesia, particularly in the field of evidence. Its evidentiary power is recognized in the ITE Law, which considers electronic information, electronic documents, and/or printouts as valid legal evidence. The validity of a digital signature can be evaluated through its implementation procedure, which uses cryptography techniques and user information to ensure its safety. The Civil Code and Article 1320 do not require specific forms or media used in transactions, which makes digital signatures a legally binding agreement as long as it meets the six conditions stated in the ITE Law Article 11 paragraph (1). The government needs to support and facilitate infrastructure and human resources development to promote the use of digital signatures and electronic

transactions in Indonesia. Furthermore, in the future, there is a need to regulate evidence in the Civil Code, which follows the development of modern technology. Overall, the digital signature plays a crucial role in ensuring efficient and secure electronic transactions and upholding the rule of law in Indonesia.

Given the growing reliance on digital signatures and electronic documents in today's society, it is important that the legal system keeps pace with these technological advancements. To ensure that justice is served, it is crucial to change our current evidentiary system and move away from a narrow, restrictive approach to evidence. This means that civil procedure law should be updated to reflect modern technology and enable the recognition and admissibility of electronic documents and digital signatures in court proceedings.

In addition, it is the responsibility of the government to create an enabling environment for the implementation of digital signatures and electronic documents. This requires investing in infrastructure and human resources, and supporting the development of technology that can facilitate the use of digital signatures and electronic documents in Indonesia. By doing so, we can ensure that our legal system is not only up-to-date, but also accessible and efficient for all stakeholders.

REFERENCES

Babbar, P., & Chandhok, S. (2008). *Paperless Society: A Digital Library Future*.

Baz, M., Alhakami, H., Agrawal, A., Baz, A., & Khan, R. A. (2021). Impact of COVID-19 Pandemic: A Cybersecurity Perspective. *Intelligent Automation & Soft Computing*, *27*(3).

Dumortier, J. (2022). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). In *EU Regulation of E-Commerce* (pp. 247–280). Edward Elgar Publishing.

Harwanto, E. R. (2022). Covers of Music and Songs Without No License Agreement of The Creator and Copyright Holder Carried Out by Corporate and Individual Black Youtubers on The Youtube Channel. *Policy, Law, Notary And Regulatory IssuesW, NOTARY AND REGULATORY ISSUES (POLRI)*, *1*(3), 81–98. https://doi.org/https://doi.org/10.55047/polri.v1i3.392

Haryanto, B., Gandhi, A., & Sucahyo, Y. G. (2020). The determinant factors in utilizing electronic signature using the TAM and TOE framework. *2020 Fifth International Conference on Informatics and Computing (ICIC)*, 1–8.

Hudzaifah, H. (2015). Keabsahan Tanda Tangan Elektronik Dalam Pembuktian Hukum Acara Perdata Indonesia. *Katalogis*, *3*(5).

Ikenwe, I. J., Igbinovia, O. M., & Elogie, A. A. (2016). Information security in the digital age: The case of developing countries. *Chinese Librarianship: An International Electronic Journal*, *42*, 16–24.

Khrykova, A., Bolsunovskaya, M., Shirokova, S., & Novopashenny, A. (2021). Implementation of digital signature technology to improve the interaction in company. *E3S Web of Conferences*, *244*, 12023.

Kie, T. T. (2000). *Studi Notariat & Serba-Serbi Praktek Notaris*. Ichtiar Baru Van Hoeve.

Kukah, A. S. K., Owusu-Manu, D.-G., & Edwards, D. (2022). Critical review of emotional intelligence research studies in the construction industry. *Journal of Engineering, Design and Technology*.

Kusmayanti, H., & Anrova, Y. (2021). Keabsahan Pembuktian Akta Notaris Di Pengadilan Sebagai Akta Otentik (Kajian Putusan No. 3591K/PDT/2018). *ADHAPER: Jurnal Hukum Acara Perdata*, *6*(2), 53–66.

Manggala, M. T. W. S., Maulana, R., Saputra, D. T., Rachmawati, I., Sumantry, D., & Trisnaningsih, M. (2021). The Role of Social Media in Promotion of Micro, Small and Medium Enterprises (MSMEs) and Its Implications Law Number 11 of 2008 Concerning Information and Electronic Transactions (UUITE). *International Journal of Latin Notary*, *2*(1), 31–39.

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258–269.

Mayasari, Y. (2022). Kedudukan Hukum Tanda Tangan Elektronik. *Jurnal Teknologi Dan Informasi*, *4*(1), 13–23.

Monteleone, S. (2015). Addressing the failure of informed consent in online data protection: learning the lessons from behaviour-aware regulation. *Syracuse J. Int'l L. & Com.*, *43*, 69.

Soekanto, S. (2007). *Normative Law research a quick review*. Raja Grafindo Persada.

White, J. (2016). Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies. *Global Security Studies*, *7*(4).

WHO. (2020). *Impact of COVID-19 on people's livelihoods, their health and our food systems Joint statement by ILO, FAO, IFAD and WH*. World Health Organization. https://www.who.int/news/item/13-10-2020-impact-of-covid-19-on-people's-livelihoods-their-health-and-our-food-systems

Wittie, R. A., & Winn, J. K. (2000). Electronic Recrods and Signatures under the Federal E-SIGN Legislation and the UETA. *Bus. Law.*, *56*, 293.

Copyrights