

Legal Study of the Validity of Electronic Signatures (digital signatures) in Business Contracts

Selvia Wisuda¹ 

¹ Universitas Merdeka Malang, Malang, Indonesia

*Corresponding author: selvia.wisuda@unmer.ac.id

Abstract

Problems in the civil sector because electronic transactions for business through electronic systems (e-commerce) have become part of domestic and international business. This shows that the correlation between the fields of informatics, media and informatics (telematics) continues to develop. Formulation of problems the status and legal strength of electronic signatures in commercial contracts and the validity of electronic signatures as evidence in the Indonesian Civil Procedure Law. Using this type of library research to collect scientific knowledge and information in the form of theories, methods or approaches that are developed and documented in the form of books, journals, manuscripts, notes, historical documents and other documents. An electronic contract is only valid if it can be ensured that all components of the electronic system can be trusted and/or function as they should.

Keywords: Signature, Electronic, Proof.

History:

Received: October 2nd 2023

Accepted: November 30th 2023

Published: December 1st 2023

Publisher: Universitas PGRI Madiun

Licensed: This work is licensed under

a [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by-sa/4.0/)



Introduction

Contracts and agreements in everyday life regulate many aspects of the economy. A contract is defined as an agreement between two or more people that binds them to do or refrain from doing something specific. (I.G Rai Widjaya, 2003) The trend in contractual legal relationships today is that these agreements are always in writing. This proves that the parties are bound by a contractual legal relationship, but does not mean that the form of an oral agreement is ruled out. (Badruzaman, 1980)

Contracts or business agreements are part of contracts and refer to business/work relationships on a large and small scale, both within the country and abroad. Its function is very important, so that it can provide legal certainty to the parties and regulate the rights and obligations of the parties, as well as secure transactions and regulate models for resolving disputes that arise between the parties. Therefore, in case of disagreement/non-performance (failure/default) of the contract between the parties, legal documents are referred to to resolve the dispute. Therefore, a contract or commercial contract is a means of ensuring that what the parties want to achieve can be realized through a contract (commercial contract).

Positive law recognizes evidence in the form of letters as written evidence. This letter is anything that contains punctuation designed to convey ideas and be used as instructions. Letters as written evidence are divided into two, namely letters which are acts and letters which are not acts. At the same time, these documents are further divided into authentic

deeds and private deeds. Making authentic deeds is the main duty and authority of a notary. (Anshori, 2009) The deed itself is a letter signed as evidence containing the events that form the basis of the contract which was made for evidentiary purposes from the start. So the letter must be signed to be classified as a deed. The requirement for a signature on a letter to be called a deed comes from Article 1869 of the Civil Code. The purpose of the signature requirement is to differentiate a deed from the words or actions of other people. (Anshori, 2009) Original documents such as notarial deeds are theoretically letters or documents that were deliberately created as official evidence. It was deliberate from the start that the writing of the letter was intended from the start to prove it later if a dispute arose, because a letter that was not intended from the start functions as evidence like ordinary correspondence. It is said to be official because it was not made by yourself but using professional services. Meanwhile, dogmatically, according to Article 1869 of the Civil Code, an authentic deed is a deed whose formation is determined by law (*welke in de ettelijke vorm is verleden*) and made by or in the presence of public servants (officials) (door of ten overstaan van openbare ambtenaren) who has the power to do so (daartoe bevoegd) at the place where the deed was made. To provide legal certainty to the parties in a work agreement (contract), perfect proof is needed in the form of a notarial deed.

The development of information technology also influences future social conditions, such as the medical care system, educational service system, public service system and many other areas of life. (Anshori, 2009) Electronic transactions are non-face (without meeting face to face), non-sign (not using an original signature) and without territorial boundaries, transactions can be carried out even in different countries) using information technology. (ITE Law, 2008) Article 1 number 19 of Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (hereinafter referred to as *PP* Government Regulation No. 82 of 2012) states that the definition of an electronic signature is a signature consisting of electronic information that is attached, associated or related to other electronic information used as a verification and authentication tool.

Regarding the validity of transactions and the strength of proof, electronic transactions do not require paper copies or paper documents, but each transaction related to their implementation has a certificate in the form of numbers or codes that can be saved or stored in a computer or printed. You can also prove the contents of a file or document, the property you want to prove is the nature of integrity, this property can be maintained and proven if a digital signature is used to verify the file, because with a digital signature, simply changing one letter in the contents of a file can show that the file is has changed, although it doesn't show which parts have changed. Realizing that various types of electronic information are very necessary in virtual operations, especially in online shop operations or often referred to as e-commerce. Digital or electronic signatures will be valid as evidence as long as they comply with the legal basis of Article 11 paragraph 1 of the ITE Law. Every person who participates in creating an electronic signature has an obligation to protect the electronic signature used. In essence, there are many advantages to identifying and managing electronic signatures, including aspects of efficiency and effectiveness. (Sulma et al, 2022)

Electronic signature security includes the following:

1. Unknown people cannot access the system.
2. The signer must follow the precautionary principle to avoid unauthorized use of information related to the electronic signature.
3. The signer must immediately use the method recommended by the electronic signature provider or notify the person by other appropriate means that the signer trusts the electronic signature or the body that supports the electronic signature service. With reason:

- a) the signer knows that the information required to create an electronic signature has been damaged; or
 - b) Circumstances known to the signatory may give rise to serious risks, which may be caused by compromise of electronic signature creation data; And
4. If an electronic certificate is used to support an electronic signature, the signatory must ensure the correctness and integrity of all information related to the electronic certificate. (Ilham, et al, 2022)

Topics that can be formulated include the status and legal power of electronic signatures in business contracts and how the validity of electronic signatures as evidence is regulated in the Indonesian Civil Procedure Law. By using this type of library research, or what is usually called normative research, the aim of conducting library research is to collect scientific knowledge and information in the form of theories, methods or approaches that are developed and documented in some form. books, journals, manuscripts, documents, historical records and other documents that can help prepare an analysis of the use of digital signatures in electronic matters, especially electronic contracts.

Materials and Methods

This research is normative research, meaning that this research examines the legal regulations themselves, not studying social phenomena as a result of existing legal regulations. The approach method used in this research is the statutory approach. This approach is used because the discussion in this research will refer to the law. The legal materials used in this paper can be divided into primary legal materials and secondary legal materials. Primary legal material is material in the form of statutory regulations that regulate and relate to the issues discussed in this research. Meanwhile, secondary legal materials are legal materials that are used to clarify primary legal materials.

Secondary legal materials Secondary legal materials are obtained from literature, scientific texts, legal writings in the form of articles and books, journals and papers, as well as legal research to find out actual legal problems, which the author considers are still closely related to the subject of this research. Methods for Collecting Legal Materials There are several ways to obtain the data used in this paper, including primary legal materials that are collected, inventoried and interpreted, to be further categorized systematically and then analyzed to answer existing problems. Secondary legal materials are used to support primary legal materials. From the collection of legal materials, processing and analysis are carried out, and the results are presented argumentatively. Analysis of Legal Materials The analysis used by the author is deductive analysis, this analysis is based on recognized legal norms, principles and values, then interpreted in a separate legal system to relate to the problems in this research.

Results and Discussion

A. The Relationship of Information Technology in Preparing Business Contract Deeds

Technology is changing many aspects of business operations and marketing. For example, in the business sector, technological developments have given rise to a business method known as electronic business (electronic business / electronic commerce). Electronic commerce is the sale and purchase of products, services and information between business partners via computer networks, namely the Internet. The internet is a "worldwide network of computer networks" or a very large computer network consisting of small networks throughout the world that are connected to each other. One of the functions of the internet is the main infrastructure for electronic commerce.

In general, according to David Baum, quoted by Onno W. Purbo and Aang Arif Wahyudi, "E-commerce is a dynamic set of technologies, applications, and business

processes that link enterprises, consumers, and communities through electronic transactions and electronic exchange of goods , services, and information”. Electronic commerce is a dynamic set of application technologies and business processes that connect businesses, consumers and specific communities through electronic commerce and the trade of goods, services and information that takes place electronically.

According to the provisions of Law of the Republic of Indonesia no. 11 of 2008 as amended by Law no. 19 of 2016 concerning Information and Electronic Transactions, Article 1 (2) states that electronic transactions are legal acts carried out using computers, computer networks and/or other electronic devices. Transaction in the Big Indonesian Dictionary means a sale and purchase agreement (in business) between two parties. From this opinion it can be concluded that the electronic goods referred to here are sales and purchase contracts carried out in business, which are carried out better and more efficiently between two/more parties via computer networks or other electronic means. Consumers are not prohibited from buying products and then reselling or purchasing the products for their own use, so electronic business (e-commerce) is subject to the business concepts contained in the Criminal Code and Civil Code. (Harris Faulidi Asnawi, 2004)

1. Mechanism for Forming Electronic Commerce Contracts (E-Commerces)

Contracting parties usually make a preliminary agreement, namely the stage before the end of the contract (agreement), which is expressed as actions taken by the parties that are agreed upon during preliminary negotiations (preliminary negotiations), at the beginning of the process, the parties agree on the conclusion of the contract.

An electronic pre-contract based on a conventional electronic or online shop is preceded by an offer to sell, an offer to buy, before the offer can be made online, for example on a website, website or mailing list and news via groups or invitations to customers through a business to business model. (Mariam Darus Badruzaman, 2001)

An offer is an offer if the other party treats or views it as an offer, that is, as an act that a person can accept as an invitation to enter into a contractual obligation. In earlier electronic contracts, especially in the commercial model, the offering party was a trader or manufacturer/seller who used a website to sell their goods and services through a kind of shop that contained a list of goods and services offered and buyers such as walking in front of the shop, shopping , browse through the window and shop anytime, anywhere regardless of distance. (Yahya Ahmad Zein, 2009)

E-commerce or electronic commerce, as it is often called, has different definitions, but in general electronic commerce refers to all types of commercial transactions involving organizations and individuals and is based on the processing and transmission of digital information, including text, voice and photographs. . (Yahya Ahmad Zein, 2009) According to Julian Ding, electronic commerce transactions are business transactions between sellers and buyers for the provision of goods and services. This contract is made on an electronic data carrier (digital data carrier), where the parties are not physically present. Using internet media or the World Wide Web. Running activities are not limited by space and time. (Julian Ding, 1999)

On the other hand, Black's Law Dictionary understands e-commerce as the practice of buying and selling goods and services on the internet. The shortened form of electronic, has become a popular prefix for other terms associated with electronic transactions. (Bryan A. Garner, 1999) According to the definition of Black's Law Dictionary, e-commerce is the practice of buying and selling goods and/or services using the internet. Based on the definition above, it can be concluded that e-commerce is all business activities involving consumers, manufacturers, service providers and intermediaries using electronic media.

E-Commerce in its application has several main characteristics that make it different from conventional commerce, Reypport and Jaworski provide several main characteristics of e-commerce, namely: (Jefrey F. Rayport & Bernard J. Jaworski, 2001)

1. E-commerce is closely related to the exchange of digital information between parties;
2. E-commerce is made possible by technology (technology enabled);
3. E-commerce uses technology as a medium (technology mediated);
4. E-commerce is related to intra- and inter-organizational activities that support the exchange process;

E-Commerce can not only be done via the internet, there are also other types of electronic transactions that can be carried out using technology other than the internet. (David Whiteley, 2000) According to Whiteley, e-commerce is divided into three types, namely Electronic Markets (EM), EDI, and Internet-Commerce. (David Whiteley, 2000)

E-Commerce can be categorized into four categories based on the subject of the relationship, namely: Business to Business (B2B), Business to Consumer (B2C), Consumer to Consumer (C2C), and Consumer to Business (C2B). (21) Business to Business (B2B) refers to e-commerce activities between companies. (B2C) refers to exchanges that occur between companies and consumers. Consumer to Consumer (C2C) refers to transactions that occur between consumers and consumers, these exchanges may or may not involve third parties, as occurs in auction exchanges via the eBay site. Lastly, Consumer to Business (C2B) refers to consumers joining together to form and establish themselves as a group of buyers for a company. (Jefrey F. Rayport & Bernard J. Jaworski, 2001)

According to Edmon Makarim, an electronic contract or online contract is: "An agreement or legal relationship that is carried out electronically by combining a network (networking) of computer-based information systems (computer based information systems) with communication systems based on telecommunications networks and services (telecommunication based) which is further facilitated by the existence of global internet computers (network of networks." (Edmon Makarim, 2003)

Based on the understanding above, it can be concluded that the conditions for the validity of a contract also depend on the nature of the electronic system itself. In other words, an electronic contract is only valid if it can be ensured that all components of the electronic system can be trusted and/or function as they should.

To date, there are four different forms of agreement in electronic contracts, namely:

1. Electronic Mail (E-Mail), is an electronic letter (email) is an electronic letter or contract made via electronic mail. Offers can be made via email to the offeree (the person receiving the offer) and offers can be accepted by sending them to the email address of the offeree
2. Shrink-wrap Contract, is a contract placed inside or on the surface of the cargo box, where usually the party who opens the cargo box is notified that he accepts the conditions stated in the contract. (the word Shrink-wrap refers to the plastic that wraps the shipping box)
3. Click-wrap Contract, is a contract that appears on the computer in the form of software and is accepted by clicking on the button. The button usually says "I Agree", "I Accept", "I Agree", etc.
4. Browse-wrap Contract, is a contract that appears on a website page in online media format and is accepted by downloading or clicking on the button. This type of contract is almost the same as a click-reel contract, only click-reel contracts can be made online. In addition, a party is deemed to have agreed if it has installed software from a website without having to click on a page on the website.

B. Support of Electronic Information Technology as a Means in the Evidence Process

With regard to the substantive legal acts that regulate electronic documents as data carriers or data carriers for electronic signatures as regulated in article 1 point 4 of the ITE Law, the term electronic document is any electronic information that is created, sent, transmitted, received or stored. analog, digital, electromagnetic, optical, etc., that can be seen, displayed, and/or heard by a computer or electronic system, including, but not limited to, text, sound, images, maps, plans, photographs, etc., letters, signs, numbers, access codes, symbols or perforations that have meaning or meaning or are understood by people who understand them. (L. Sihombing, 2020) The status of electronic documents as evidence is regulated in article 5 (1) of the ITE Law, which reads:

Article 5 (1)

That the existence of Electronic Information and/or Electronic Documents is binding and recognized as valid evidence to provide legal certainty regarding the Implementation of Electronic Systems and Electronic Transactions, especially in evidence and matters relating to legal actions carried out through Electronic Systems.

1. The existence of Information Technology in Making Electronic Signatures

To achieve the purpose of signing electronic documents, the signature must have the following characteristics:

- a) Signature authentication The signature must identify the person signing the document and must be difficult for others to imitate.
- b) Authentication of documents: The signature must identify the signer, which makes it impossible to forge or change it (both the signed document and the signature) without being noticed.

Through the concept of "nonrepudiation" to avoid falsification in the field of information security. Nonrepudiation is a guarantee of the authenticity or delivery of an original document to avoid rejection by the signer of the document (that he did not sign the document) and by the sender of the document (that he did not send the document).

Creating digital signatures uses cryptographic techniques, which is a branch of applied mathematics that deals with the transformation of data into another form that cannot be understood and returned to its original state. Digital signatures use "public key cryptography", if an algorithm uses two keys, the first key is used to generate a digital signature or to convert data to another form that cannot be understood, and the second key is used to verify the signature digital or restore the message to its original form. This concept is also known as "asymmetric cryptosystem" (non-symmetric cryptographic system). This encryption system uses a private key known only to the signer, which is used to create a digital signature, and a public key, which is used to verify the digital signature. If multiple people want to verify a person's digital signature, the public key must be shared between them. Private keys and public keys are actually "related" mathematically (according to certain equations and rules). However, the private key cannot be found using information from the public key. Another equally important process is the "hash function" used to create and verify digital signatures. A hash function is an algorithm that creates a digital representation or a kind of "fingerprint" in the form of a "hash value" and is usually much smaller than the original document and unique only to that document. Even the smallest change in a document results in a change in the "hash value" correlated with that document. Such a hash function is also called a "one-way hash function" because the hash value cannot be used to modify the original document.

Therefore, a hash function can be used to generate a digital signature. This hash function creates a "fingerprint" of the document (so it is unique only to that document) that is much smaller than the original document and can detect if the document has been changed

from its original form. Using a digital signature requires two processes, namely the signer and the recipient. In detail these two processes can be explained as follows:

1. Create a digital signature using the generated hash value of the document and a predefined private key. To ensure the security of a hash, there must be a very small probability that the same digital signature can be created from two different documents and private keys.
2. Digital signature verification is the process of verifying a digital signature by referring to the original document and the public key provided, which determines whether the digital signature created on the same document using the private key matches the public key.

To sign a document or other piece of information, the signer first determines exactly which parts to sign. This limited information is called "message". The digital signature application then generates the hash value into a digital signature using the private key. The resulting digital signature is unique to the message and private key. Typically, a digital signature is added to a document and is also stored with the document. However, a digital signature can be sent or saved as a separate document if it can be attached to the document. Since digital signatures are unique within a document, such separation of digital signatures is not necessary. The process of creating and verifying digital signatures fulfills the basic elements necessary to achieve legitimate objectives, namely:

- a) Signer verification: If a public key and private key pair are associated with a specific legal owner, a digital signature can be used to add or attach a document to the signer. Digital signatures cannot be forged unless the signer loses control of their private key.
- b) Document authentication: a digital signature identifies the document to be signed with much greater certainty and precision than a paper signature.
- c) Requirements: The signer's private key is required to create a digital signature. This action can confirm that the signer accepts the document and is responsible for it.
- d) Efficiency: The process of creating and verifying digital signatures provides a high level of assurance that the existing signature is a valid and authentic signature of the private key owner. In the case of a digital signature, there is no need to carefully check (verify) the signature contained in the document with a sample of the original signature, as is usually done when checking the signature manually.

The purpose of a signature on a document is to ensure the authenticity of the document. A digital signature is not actually a signature as it is known today, but uses a different way of marking a document so that the document or information not only identifies the sender, but also ensures that the integrity of the document is not changed during the processing or transmission process. The digital signature is based on the content of the message itself.

To electronically sign a message, the sender first uses software to create a message digest 16 summary of the original letter using the fonction de hachage (hash in English). The message digest of each original message is as unique as its "fingerprint", so the slightest change in the message digest will result in a change in its "fingerprint". The advantage is that both the sender and recipient can know the integrity of the message. Additionally, the message digest is signed with the sender's private key, e.g. An electronic signature is a message digest encrypted with the sender's private key.

The original message and electronic signature are then sent together to the desired destination. Thanks to the sender's public key, which is sent to the recipient of the message in advance, the recipient can decipher the electronic signature, saying that the result is A1, then the recipient creates a message digest from the originally received message, saying that the result is A2. Then the final step is to compare the two, namely A1 and A2. If both have the

same "fingerprint", you can be sure that the message is genuine and has not been altered. However, this process cannot verify the identity of the message creator.

2. Strength of Proof of Electronic Signatures in Business Contracts According to Civil Procedure Law

BW (Burgerlijk Wetboek or Civil Code or Buk uke four), contains the basis for civil evidence. In terms of evidence related to the case. Legal experts have provided several definitions that can be used as a reference. According to Pitlo, proof is a method used by a party to establish facts and rights related to its interests. According to Subekti, what is meant by "prove" is to convince the judge of the truth of the argument or arguments put forward in a dispute.

There is a difference between scientific evidence and law. Scientific evidence defines truth for everyone, but evidence presented in court (case) is only for the people concerned and their legitimate descendants. As regulated in laws 164 HIR (283 RBG) and 1903 BW, it is known that there are only 5 (five) types of evidence that can be submitted to court, especially in civil cases, including:

1. Written proof
2. Evidence with witnesses
3. Estimates
4. Recognition
5. Oath

Digital signatures as electronic information in this case are problematic when presented as evidence in the trial process in Indonesia. Digital signatures used in e-commerce are completely paperless, they are not even written. According to the provisions of this article, this means that evidence sent in the form of electronic information is not considered as evidence. There is also a high probability that the case will be rejected as evidence by the judge or opposing party. (Selviaco, 2022)

In this case, existing and applicable statutory regulations (positive procedural law) must be revised because of this urgent need. The e-commerce problem is before our eyes and the possibility of disputes is only a matter of time. If this happens, one suspects that difficult evidentiary problems will arise. The problems mentioned above are only part of the whole problem.

Pitlo, a Dutch legal scholar grouped them in order of strength:

1. Authentic Deed
2. Underhand Deed
3. Not a Deed

In court, to obtain full evidentiary rights, it is appropriate to provide authentic documentary evidence when presenting a fact. A digital signature must have the same evidentiary power as an authentic document.

Therefore, if we want to apply a digital signature as an attachment so that it has the same legal force as an authentic document, there are problems that must be resolved. First, the writing side. Second, it is carried out by or in the presence of an authorized official or public official.

Conclusion

1. The status and legal force of electronic signatures (Digital Signature) in electronic contracts plays a very important role. As proof that the parties who sign a contract or commercial contract agree on the contents of the contract and the legal consequences that may arise from the negligence of one of the parties. A signature is one of the conditions that must be in the contract.

2. The validity of electronic signatures as evidence within the meaning of the Indonesian Civil Procedure Law is recognized in principle after being regulated by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Electronic Information or Electronic Document Transactions. It is valid evidence and an extension of legal evidence according to procedural law in Indonesia. This is based on the provisions of Article 5 (2) that valid evidence consists of written evidence, witness evidence, accusations, confessions and written statements. Thus, the form of electronic data/electronic documents mentioned above is formalized in the Process Law and electronic data or electronic documents themselves are valid evidence according to the Information and Electronic Transactions Law.

Acknowledgments

The researcher would like to thank my friends who helped me complete this research:

References

- Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions
- Government Regulation Number 82 of 2012 concerning Implementation of Electronic Systems and Transactions
- Abdul Ghofur Anshori, 2009, Lembaga Kenotariatan Indonesia Perspektif Hukum dan Etika, Yogyakarta: UII Press
- Agus Yudha Hernoko, 2011, Hukum Perjanjian Asas Proporsionalitas dalam Kontrak Komersil, Jakarta: Kencana
- Arrianto Mukti Wibowo, 1999, Kerangka Hukum Digital Signature Dalam Electronic Commerce, amwibowo@caplin.cs.ui.ac.id
- Bryan A. Garner, 1999 Black's Law Dictionary, Minnesota: West Group
- David Whiteley, 2000, E-Commerce: Strategy, Technologies, and Applications, London: McGraw Hill International
- Edmon Makarim, 2003, Kompilasi Hukum Telematika, Jakarta: Raja Grafindo Persada
- Falahiyati, N. (2020). Tinjauan Hukum Kontrak Elektronik Dalam Pinjam Meminjam Uang Berbasis Teknologi Informasi (Transaksi Peer To Peer Lending). *Jurnal Justiqua*, 2(1), 1-11.
<http://www.portaluniversitasquality.ac.id:5388/ojsystem/index.php/JUSTIQA/article/view/325> DOI: <http://dx.doi.org/10.36764/justiqua.v2i1.325>
- Haris Faulidi Asnawi, 2004, Transaksi Bisnis E-commerce Perspektif Islam, Yogyakarta, Magistra Insania Press bekerjasama dengan MSI MUI
- I.G Rai Widjaya, 2003, Merancang Suatu Kontrak, Jakarta: Kesaint Blanc
- Jefrey F. Rayport dan Bernard J. Jaworski, 2001, E-Commerce, Singapura: McGraw- Hill

- Jeremy G.Thorn, 1995, Terampil Bernegosiasi ,alih bahasa Edi Nugroho, Jakarta: Pustaka Binaman Pressindo
- Julian Ding, 1999, E-Commerce: Law & Practice, Malaysia: Sweet & Maxwell Asia
- Khairatus Sulma, Jamaluddin Jamaluddin, Arif Rahman, Keabsahan Tanda Tangan Elektronik dan Kekuatan Pembuktiannya dalam Hukum Acara Perdata, Jurnal Ilmiah Mahasiswa Fakultas Hukum Universitas Malikussaleh, Vol 5, No 3 (2022), <https://ojs.unimal.ac.id/jimfh/article/view/7107> DOI: <https://doi.org/10.29103/jimfh.v5i3.7107>
- L. Sihombing, “KEABSAHAN TANDA TANGAN ELEKTRONIK DALAM AKTA NOTARIS”, JURNAL EDUCATION AND DEVELOPMENT, vol. 8, no. 1, p. 134, Jan. 2020. DOI <https://doi.org/10.37081/ed.v8i1.1515> <https://journal.ipts.ac.id/index.php/ED/article/view/1515>
- Mariam Darus Badruzaman, 1980, Pelangi Perdata II, Medan: Fakultas Hukum Universitas Sumatera Utara
- Mariam Darus Badruzaman, 2001, E-Commerce: Tinjauan dari hukum kontrak Indonesia, Jurnal Hukum Bisnis, XII.
- R. Subeksi, R. Tjitrosudibio, 2004, Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek), Jakarta : PT. Pradnya Paramita
- Selvia Wisuda, Perlindungan Hukum Konsumen Pengguna e-Banking: Ditinjau dari Undang-Undang Perlindungan Konsumen dan Undang-Undang Perbankan, Merdeka Law Journal, Vol 3, No 1 (2022), DOI: <https://doi.org/10.26905/mlj.v3i1.9176>
- Yahya Ahmad Zein, 2009, Kontrak Elektronik & Penyelesaian Sengketa Bisnis E-Commerce dalam Transaksi Nasional dan Internasional, Bandung: CV. Mandar Maju