International Journal of Educational Review, Law & Social Sciences (IJERLAS)
International Journal of Educational Review, Law And Social Sciences (IJERLAS Journal) | ISSN(e): 2808-487X
Volumes 5 No. 6 (2025)

VALIDITY OF ELECTRONIC AGREEMENTS WITH DIGITAL SIGNATURES FROM THE PERSPECTIVE OF INDONESIAN CIVIL LAW

Naib[1]
Universitas Pamulang[1]
Email: dosen02103@unpam.ac.id

Received :01 November 202
Revised :15 November 2025
Accepted :10 December 2025
Published : 16 January 2026
DOI : https://doi.org/10.54443/ijerlas.v5i6.4965
Link Publish : https://radjapublika.com/index.php/IJERLAS

Abstract

This study analyzes the validity of electronic agreements with digital signatures from the perspective of Indonesian civil law, based on the Civil Code (KUHPerdata) and related regulations such as Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE). Using a normative legal research method with a statutory and conceptual approach, this study discusses the fulfillment of the valid requirements of an agreement according to Article 1320 of the Civil Code, namely agreement, capacity, certain things, and lawful cause, in an electronic context. Digital signatures, which utilize cryptography for authentication, integrity, and non-repudiation, are recognized as valid if they meet the requirements of Article 11 of the ITE Law, especially those certified by an Electronic Certification Provider. In addition, the evidentiary power of digital signatures as an extension of written evidence (Article 5 of the ITE Law) varies; certified signatures have a higher authentic value than uncertified ones. The conclusion states that electronic agreements are valid and have legal certainty, although there are limitations for certain formal documents, and recommends the use of certified signatures to reduce the risk of civil disputes.

Keywords: Electronic Agreement, Digital Signature, Indonesian Civil Law.

INTRODUCTION

Developments in information and communication technology (ICT) have brought significant changes to several aspects of life, including the legal field. One of the most striking changes is the emergence of electronic agreements (e-contracts). An electronic agreement is an agreement made electronically, that is, using electronic means, such as email, websites, or mobile applications. Electronic agreements have become an integral part of modern society today. (Mahesa, 2023) Article 1313 of the Civil Code states that " a contract or agreement is an act by which one or more people bind themselves to one or more people ." (Hernoko & Agus, 2014)According to Subekti, the definition of an agreement is where one person promises to another person or where two people promise each other to do something. (Subekti, 1979)Article 1320 of the Civil Code stipulates four conditions for a valid agreement, namely: (1) agreement of those who bind themselves; (2) capacity to make an agreement; (3) a certain thing; and (4) a lawful cause. In the context of electronic agreements, fulfilling these conditions faces its own challenges, especially related to the aspects of agreement and capacity of the parties who do not meet in person.

One of the important elements in an electronic agreement is a digital signature . A signature is proof of authentication or verification of a person's identity which is one of the proofs of the authenticity or validity of an agreement or consent on something in a document carried out by two or more parties. (Slamet & Pailing, 2019)Unlike conventional signatures which are manually affixed on paper, a digital signature is the result of cryptographic techniques that function to verify the identity of the signatory and guarantee the integrity of electronic documents. Article 1 number 12 of the ITE Law defines an electronic signature as " a signature consisting of Electronic Information attached, associated or related to other Electronic Information used as a means of verification and authentication ". The existence of this digital signature is crucial because it functions to replace the role of a wet signature in providing approval and identification of the parties in an agreement. A digital signature has the same purpose as a wet/physical signature, which is to prove that the document is original and valid. (Dahlia & Susetio, 2023)Digital signatures and electronic signatures are two different things. This difference is clearly visible in terms of security, authenticity, validity, and confidentiality of the signature owner's data. (Ponorogo, n.d.)Article 1 number 12 of the Electronic Information and Transactions Law (hereinafter referred to as the ITE Law) states that " An

electronic signature is a signature consisting of Electronic Information attached, associated or related to other Electronic Information used as a means of verification and authentication. " An electronic signature refers to data in its electronic form, which is attached to an electronic document. This data is electronic information from the signing and its form is not limited to wet (handwritten) signatures made into electronic form. Meanwhile, a digital signature is a cryptographic mechanism that is often implemented into electronic signatures. (Dermawan, 2021) Although the development of digital technology has been accommodated in Indonesian laws and regulations, particularly through the ITE Law and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), there are still questions regarding the validity of electronic agreements that use digital signatures when evaluated based on the provisions of agreement law regulated in the Civil Code (KUHPerdata).

Another issue that arises is regarding the evidentiary power of digital signatures in electronic agreements. Article 1866 of the Civil Code regulates valid evidence in the law of evidence, which traditionally includes written evidence, witnesses, allegations, confessions, and oaths. The emergence of electronic documents and digital signatures as new evidence requires an in-depth study of their evidentiary power, especially in the event of a dispute between the parties. Article 5 paragraph (1) of the ITE Law states that " Electronic Information and/or Electronic Documents and/or printouts thereof constitute valid legal evidence ", but how this is concretely implemented in civil court practice still requires a comprehensive understanding. Based on the above background, this study aims to analyze two main issues. First, how is the validity of electronic agreements using digital signatures reviewed from the perspective of the valid requirements of an agreement according to the Civil Code and related laws and regulations in Indonesia? Second, how evidentiary is the digital signature in electronic agreements in the event of a civil dispute between the parties. This issue is important to examine to provide legal certainty for the public, who are increasingly using electronic agreements in various transactions, both in business and other civil contexts.

RESEARCH METHODS

This research uses a normative legal research method (doctrinal research) with a statute approach and a conceptual approach . Normative legal research is research conducted by reviewing and analyzing legal materials related to the problem being studied. The legal materials used in this study consist of primary legal materials and secondary legal materials. Primary legal materials include the Civil Code, Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, Government Regulation Number 80 of 2019 concerning Commerce Through Electronic Systems, and Regulation of the Minister of Communication and Informatics Number 11 of 2018 concerning the Implementation of Electronic Certification. Secondary legal materials used include textbooks, scientific journals, articles, and research results relevant to the research topic. The legal materials collection technique is carried out through library research by collecting, classifying, and analyzing relevant legal materials. The analysis of legal materials is carried out qualitatively with a descriptive-analytical method, namely describing the applicable laws and regulations and then analyzing them in the context of the problem being studied. A systematic approach is used to find the relationship between various laws and regulations governing electronic agreements and digital signatures, as well as to identify the conformity and gaps between the provisions of the Civil Code and the regulations in the ITE Law and its implementing regulations.

RESULTS AND DISCUSSION

The Validity of Electronic Agreements with Digital Signatures Reviewed from the Validity Requirements of Agreements

The validity of an agreement in Indonesian civil law is based on the provisions of Article 1320 of the Civil Code which regulates four conditions for a valid agreement, namely: (1) agreement of those who bind themselves; (2) capacity to make an agreement; (3) a certain thing; and (4) a lawful cause. The first two conditions are called subjective conditions because they relate to the subject or parties who make the agreement, while the last two conditions are called objective conditions because they relate to the object of the agreement. Failure to fulfill subjective conditions causes the agreement to be voidable , while failure to fulfill objective conditions causes the agreement to be null and void . (Subekti, 1979)

In the context of electronic agreements that use digital signatures, the fulfillment of these four conditions has different characteristics from conventional agreements. The first condition, namely the agreement of the parties, in electronic agreements is realized through a point and click or browsewrap agreement mechanism where the parties state their agreement by clicking the "agree" or " accept " button on the electronic platform. (Sukarmi, 2008)According to the provisions of Article 47 paragraph (2) of the PP PSTE, " Electronic Transactions occur at the

time of agreement between the parties ." Agreement in electronic transactions can be known from the confirmation of acceptance sent by the party receiving the offer to the party making the offer.

The terms of agreement in an electronic agreement must meet the same principles as a conventional agreement, namely freedom from coercion (dwang), error (dwaling), and fraud (bedrog) as stipulated in Article 1321 of the Civil Code. In practice, the principle of take it or leave it is often applied in electronic agreements, where one party (usually the service provider) has provided an agreement template and the other party can only accept or reject it without any room for negotiation. However, as long as the party accepting the agreement does so consciously and without any flawed will, the agreement remains legally valid. The second requirement is the parties' capacity to enter into a contract. Article 1329 of the Civil Code states that every person is competent to enter into a contract, except those declared incompetent by law, namely minors and those placed under guardianship. In electronic agreements, the issue of capacity becomes more complex because the parties do not meet in person. Article 2 of the ITE Law states that this law applies to "every person" who performs a legal act, but does not provide explicit limitations or mechanisms for verifying age and legal capacity.

To address the issue of verifying competence in electronic agreements, the Explanation of Article 9 of the ITE Law states that business actors offering products through electronic systems must provide complete and correct information, including information containing the identity and status of legal subjects and their competence. (Penjelasan Pasal 9 UU No. 11 Tahun 2028 tentang Informasi dan Transaksi Elektronik)Furthermore, the provisions of Article 64 paragraph (1) of the PP PSTE stipulate that before an electronic signature is used, the Electronic Certification Provider must ensure the initial identification of the signatory by: (a) the signatory submitting its identity to the Electronic Certification Provider; (b) the signatory registering with the Electronic Certification Provider; and (c) if necessary, the Electronic Certification Provider may confidentially transfer the signatory's identity data to another Electronic Certification Provider with the signatory's consent.

The identity verification mechanism by the Electronic Certification Provider (PSrE) is crucial to ensuring that parties signing electronic agreements are legally competent. The verification process can include checking identity documents such as National Identity Cards (KTP), biometric verification, or other authentication methods. Therefore, a certified digital signature provides a stronger guarantee that competency requirements have been met compared to electronic agreements that use scanned signatures without verification. The third requirement is the existence of a specific item that is the object of the agreement. Article 1333 of the Civil Code stipulates that an agreement must have a principal item whose type can at least be determined. In electronic agreements, the object of the agreement can be a physical item or a digital item such as software , digital content, or services provided through an electronic platform. Article 9 of the ITE Law stipulates the obligation of business actors to provide complete information about the products offered, including "the name, address, and description of the goods/services." This provision ensures that the requirement for a specific item can be met in electronic agreements.

The fourth requirement is the existence of a lawful cause. Article 1337 of the Civil Code states that a cause is prohibited if it is contrary to law, morality, and public order. In the context of electronic agreements, it is important to ensure that the transactions carried out do not involve goods or services prohibited by statutory regulations. Article 17 paragraph (2) of the PP PSTE stipulates that parties conducting electronic transactions must act in good faith in interacting and/or exchanging electronic information during the transaction. This principle of good faith reflects the need to fulfill the requirement of a lawful cause in electronic agreements. Regarding digital signatures, Article 11 paragraph (1) of the ITE Law stipulates that electronic signatures have legal force and valid legal consequences as long as they meet certain requirements. The full quote from the article mentions six requirements, namely: "(a) the data for creating an Electronic Signature is related only to the Signatory; (b) the data for creating an Electronic Signature during the electronic signing process is only under the control of the Signatory; (c) any changes to the Electronic Signature that occur after the time of signing can be identified; (d) any changes to the Electronic Information related to the Electronic Signature after the time of signing can be identified; (e) there is a specific method used to identify who the Signatory is; and (f) there is a specific method to show that the Signatory has given approval to the related Electronic Information."

These requirements demonstrate that a digital signature is more than just a scan of a wet signature; it must also possess authentication, integrity, and non-repudiation functions . Authentication ensures that the signature truly comes from the party claiming to be the signer. Integrity ensures that the signed document remains unchanged after signing. Non-repudiation prevents the signer from denying their signature. These three functions can only be fulfilled through the cryptographic technology implemented in a certified digital signature. (Prabowo & Afrianto, 2017) Furthermore, Article 60 paragraph (2) of the PSTE PP distinguishes between certified and uncertified electronic signatures. Certified electronic signatures must use electronic certification created by an Indonesian Electronic Certificate Provider and use a certified electronic signature creation device. Meanwhile, uncertified electronic signatures are

created without using the services of an electronic certificate provider. This distinction has significant legal implications for the validity and evidentiary power of electronic agreements.

Probative Power of Digital Signatures in Electronic Agreements

The evidentiary power of a document in Indonesian civil procedural law is regulated in Article 1866 of the Civil Code, which states that evidence consists of: (1) written evidence; (2) evidence with witnesses; (3) allegations; (4) confessions; and (5) oaths. In the context of electronic agreements, electronic documents and digital signatures fall into the category of written evidence that is specifically recognized by the ITE Law as an extension of valid evidence. Article 5 paragraph (1) of the ITE Law expressly states that " Electronic Information and/or Electronic Documents and/or printouts thereof constitute valid legal evidence ." This provision is reinforced by Article 5 paragraph (2) which states that " Electronic Information and/or Electronic Documents and/or printouts thereof as referred to in paragraph (1) constitute an extension of valid evidence in accordance with the applicable Procedural Law in Indonesia ." Thus, electronic documents containing agreements with digital signatures have the status of valid evidence in the Indonesian evidentiary legal system.

However, not all electronic information and electronic documents can be directly accepted as valid evidence. Article 5 paragraph (4) of the ITE Law excludes: "(a) letters which according to the law must be made in written form; and (b) letters and documents which according to the law must be made in the form of a notarial deed or a deed made by a deed-making official ." This exception is important for understanding the limits of the use of electronic documents in Indonesian legal practice, where for certain documents which require special formalities, electronic documents cannot yet completely replace physical documents. (Kusumaningrum, 2011) To be accepted as valid evidence, electronic documents must meet the requirements stipulated in Article 6 of the ITE Law, namely: " In the event that there are provisions other than those stipulated in Article 5 paragraph (4) which require that information must be in written or original form, Electronic Information and/or Electronic Documents are deemed valid as long as the information contained therein can be accessed, displayed, its integrity guaranteed, and can be accounted for so that it explains a situation ." This requirement emphasizes the aspects of accessibility, integrity, and accountability of electronic documents.

In the Explanation of Article 5 of the ITE Law as amended by Law Number 19 of 2016, it is stated that " the existence of Electronic Information and/or Electronic Documents is binding and recognized as valid evidence to provide legal certainty for the Implementation of Electronic Systems and Electronic Transactions, especially in evidence and matters relating to legal acts carried out through Electronic Systems ." This explanation emphasizes that electronic documents are not only formally recognized as evidence, but also have binding power and provide legal certainty. (Sari, 2022) Regarding the evidentiary power of digital signatures specifically, Article 11 of the ITE Law stipulates that electronic signatures have legal force and valid legal consequences as long as they meet the aforementioned requirements. However, the level of evidentiary power of digital signatures varies depending on the type of electronic signature used. As explained in the Explanation of Article 54 of the PP PSTE, " the legal consequences of using certified or uncertified Electronic Signatures affect the strength of their evidentiary value ."

Certified electronic signatures issued by Electronic Certification Providers (PSrE) recognized by the Ministry of Communication and Informatics have stronger evidentiary power. (Putri & Wisnaeni, 2023)This is because the electronic certificate issuance process involves rigorous identity verification, the use of secure cryptographic technology, and a reliable authentication mechanism. In contrast, uncertified electronic signatures, such as scanned wet signatures affixed to electronic documents, have weaker evidentiary power because they are vulnerable to forgery and lack adequate verification mechanisms. (Listyana, Wati, & Lisnawati, 2014) In judicial practice, when a dispute arises regarding an electronic agreement using a digital signature, the judge will assess the evidentiary strength of the document based on several factors. First, the judge will examine whether the digital signature meets the technical requirements as stipulated in Article 11 of the ITE Law. Second, the judge will consider whether the digital signature was issued by a government-recognized PSrE. Third, the judge will assess the integrity of the electronic document, namely whether the document has been altered since it was signed. Fourth, the judge may request expert testimony (expert witness) to verify the validity of the digital signature and the integrity of the electronic document. (Putri & Wisnaeni, 2023)

In the event of repudiation by a party claiming never to have signed an electronic document, the burden of proof will vary depending on the type of signature used. For certified digital signatures, the denying party has a heavier burden of proof because it must prove that the electronic certification system has been compromised or that the private key used has been stolen or misused by another party without its knowledge. (Andalan, 2019)Conversely, for simple electronic signatures without certification, the party alleging the validity of the signature has a heavier burden of proof to show that the signature was actually created by the relevant party. (Listyana, Wati, & Lisnawati, 2014) It should be noted that Article 49 paragraph (3) of Government Regulation Number 80 of 2019 concerning

Trading Through Electronic Systems (PP PMSE) provides special recognition for certified electronic signatures by stating that " Proof of transactions using certified or parent Electronic Signatures can be considered as authentic written evidence ." This provision indicates that certified electronic signatures can be equated with authentic deeds in terms of their evidentiary power, although it is still necessary to pay attention to the restrictions stipulated in Article 5 paragraph (4) of the ITE Law regarding documents that must specifically be made in the form of a notarial deed. In the context of dispute resolution, parties who use electronic agreements with digital signatures can resolve disputes through litigation or non-litigation channels. For litigation channels, parties can file a lawsuit with the district court in accordance with the provisions of HIR (Het Herziene Indonesisch Reglement) or RBg (Rechtsreglement voor de Buitengewesten). (Usman, 2020)Article 38 paragraph (1) of the ITE Law specifically stipulates that " Any person can file a lawsuit against a party that organizes an Electronic System and/or uses Information Technology that causes losses ." In the trial process, electronic documents and digital signatures can be submitted as written evidence in accordance with the provisions of Article 5 of the ITE Law. For non-litigation routes, Article 39 paragraph (1) and (2) of the ITE Law stipulates that " Civil lawsuits are conducted in accordance with the provisions of the Laws and Regulations " and " In addition to the settlement of civil lawsuits as referred to in paragraph (1), the parties may resolve disputes through arbitration, or other alternative dispute resolution institutions in accordance with the provisions of the Laws and Regulations ." The choice of settlement through arbitration or Alternative Dispute Resolution (ADR) such as mediation and negotiation is often chosen because it is more efficient in terms of time and costs, and provides better confidentiality for the parties. (Sari, 2022)

CONCLUSION

Based on the analysis of the issues discussed, two main conclusions can be drawn. First, electronic agreements using digital signatures can be declared valid under Indonesian civil law as long as they meet the requirements for a valid agreement as stipulated in Article 1320 of the Civil Code, which include agreement of the parties, capacity to enter into an agreement, the existence of certain matters, and a lawful cause. In the context of electronic agreements, fulfilling these requirements requires special mechanisms such as identity verification by an Electronic Certification Provider (PSrE), the use of cryptographic technology to ensure document integrity, and the clarity of the object and cause of the agreement. Certified digital signatures issued by a government-recognized PSrE provide a stronger guarantee of fulfilling these requirements compared to simple, uncertified electronic signatures. The relationship between the provisions of the Civil Code and the regulations in the ITE Law and the PP PSTE shows that the Indonesian legal system has accommodated the development of digital technology in the realm of civil agreements, although there are still limitations for certain documents that require special formalities.

Second, the evidentiary force of digital signatures in electronic agreements is legally recognized by the ITE Law as an extension of written evidence in Indonesian civil evidence law. However, the level of evidentiary force varies depending on the type of electronic signature used. Certified digital signatures have the same evidentiary force as authentic written evidence because they meet the authentication, integrity, and non-repudiation requirements stipulated in Article 11 of the ITE Law. Conversely, uncertified electronic signatures have weaker evidentiary force because they are vulnerable to forgery and lack adequate verification mechanisms. In judicial practice, judges will assess the validity of digital signatures based on their fulfillment of technical requirements, the credibility of the PSrE issuing the certificate, and the integrity of the electronic document. Disputes related to electronic agreements can be resolved through litigation in court or non-litigation through arbitration or Alternative Dispute Resolution (ADR), with electronic documents and digital signatures as valid evidence in accordance with applicable laws and regulations.

REFERENCES

Andalan, A. M. (2019). Kedudukan Tanda Tangan Elektronik dalam Transaksi Teknologi Finansial. Jurist-Diction, 2(6), 1931-1950.

Dahlia, M., & Susetio, W. (2023). Tinjauan Yuridis Penggunaan Tanda Tangan Digital dalam Perjanjian Jual Beli . Jurnal Multridisiplin Indonesia, 2(8), 2277-2289.

Dermawan, R. (2021). Pemanfaatan Tanda Tangan Digital Tersertifikasi di Era Pandemi. Rewang Rencang: Jurnal Hukum Lex Generalis, 2(8), 762-781.

Hernoko, Y., & Agus. (2014). Hukum Perjanjian atas Proporsionalitas dalam Kontrak Komersial. Jakarta: Kencana.

Kusumaningrum, E. (2011). Keabsahan Kontrak Elektronik dalam UU ITE Ditinjau dari Pasal 1320 KUHPerdata dan UNCITRAL Model Law on Electronic Commerce. Risalah Hukum, 64-76.

Lapian, R., Soeikromo, D., & Mamengko, R. S. (2024). Pengaturan Penggunaan Tanda Tangan Elektronik Menurut UU No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. Lex Privatum, 13(1).

Listyana, D. S., Wati, I. A., & Lisnawati. (2014). Kekuatan Pembuktian Tanda Tangan Elektronik Sebagai Alat Bukti yang Sah Dalam Perspektif Hukum Acara di Indonesia dan Belanda. Verstek, 2(2), 146-154.

Mahesa, B. T. (2023). Keabsahan Perjanjian Elektronik Penyedia Layanan Uang Digital (Studi Kasus Hilangnya Uang di Aplikasi Dana). Sains Student Research, 1(1), 1087-1093.

Makarim, E. (2014). Notaris dan Transaksi Elektronik: Kajian Hukum Tentang Cybernotary atau Elektronik Notary. Jakarta: PT. Raja Grafindo Persada.

Penjelasan Pasal 9 UU No. 11 Tahun 2028 tentang Informasi dan Transaksi Elektronik. (n.d.).

Ponorogo, D. K. (n.d.). Tanda Tangan Elektronik vs Tanda Tangan Digital. Retrieved from https://kominfo.ponorogo.go.id/tanda-tangan-elektronik-vs-tanda-tangan-digital

Prabowo, E. C., & Afrianto, I. (2017). Penerapan Digital Signature dan Kriptografi Pada Otentikasi Sertifikasi Tanah Digital. Jurnal Ilmiah Komputer dan Informatika (KOMPUTA), 6(2), 2089-9033.

Putri, A. R., & Wisnaeni, F. (2023). Kekuatan Pembuktian dan Penyelesaian Sengketa Penggunaan Tanda Tangan Digital dalam Perjanjian. NOTARIUS, 16(2), 948-959.

Sari, I. P. (2022). Keabsahan Perjanjian Kontrak Elektronik dalam Transaksi E-Commerce Ditinjau dari Hukum Perdata. Jurnal Al-Wasath, 3(2), 105-112.

Slamet, T., & Pailing, M. (2019). Kekuatan Hukum Transaksi dan Tanda Tangan Elektronik dalam Perjanjian. Paulus Law Journal, 1(1), 9-18.

Subekti, R. (1979). Hukum Perjanjian. Jakarta: Intermasa.

Sukarmi. (2008). Kontrak Elektronik dalam Bayang-Bayang Pelaku Usaha. Bandung: Pustaka Sutra.

Usman, T. (2020). Keabsahan Tanda Tangan Elektronik Pada Perjanjian Jual Beli Barang dari Prespektif Hukum Perdata. Indonesian Privat Law, 1(2), 87-98.

Yuniati, T., & Sidiq, M. F. (2021). Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi. Jurnal Resti (Rekayasa Sistem dan Teknologi Informasi). 4(6), 1058-1069.

PERATURAN PERUNDANG-UNDANGAN

Kitab Undang-Undang Hukum Perdata.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185.

Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 222.

Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik. Berita Negara Republik Indonesia Tahun 2018 Nomor 1238.