International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 08 Issue 05 May 2025

DOI: 10.47191/ijsshr/v8-i5-04, Impact factor- 8.007

Page No: 2664-2669

Authentication of Electronic Signatures in Online Business Transactions

I Gusti Ayu Andara Yadnya Sangaswary[1], Ketut Kasta Arya Wijaya[2], Putu Ayu Sriasih Wesna[3]

[1]Students of the Master of Notary Postgraduate Program at Warmadewa University

[2,3]Warmadewa University Faculty of Law

ABSTRACT: Technological developments have driven digitalization in online business transactions, including the use of electronic signatures (ETS) as a substitute for conventional signatures. Although ETS have been legally recognized in the Electronic Information and Transactions Law (UU ITE), there is still debate regarding their authentication, legal force, and legal protection. This study aims to analyze the authentication regulations and legal force of ETS from the perspective of positive Indonesian law using normative methods through legislative and conceptual approaches. The results of the study show that ETS authentication is based on the ITE Law and asymmetric cryptography technology with public key infrastructure. Certified ETS have stronger legal force because they are supported by Electronic Certification Organizers (PSrE) supervised by the Ministry of Communication and Information. The authentication process involves registration, identity verification, and issuance of electronic certificates by PSrE. The government provides legal protection through strict regulations and criminal sanctions for forgery of ETS. With clear regulations, certified ETS have legal force equivalent to manual signatures and can be used as valid evidence in court. To increase trust in digital transactions, it is necessary to socialize the use of certified ETS and improve regulations and procedures for issuing electronic certificates. Further research with an empirical approach is needed to understand the effectiveness and application of TTE in various business sectors.

KEYWORDS: Electronic Signature (TTE), Authentication, Legal Power, Online Business Transactions, Electronic Certification Organizers (PSrE)

I. INTRODUCTION

A signature serves as a written representation of an individual's identity and functions as evidence of the authenticity and legal validity of a document. The legal framework governing signatures is stipulated in the Indonesian Civil Code, specifically in Book Four, Chapter II on Documentary Evidence (Articles 1867–1894). Article 1875 of the Civil Code outlines the evidentiary value of a signature, stating: "A private deed that is acknowledged as authentic by the person against whom it is presented, or is legally deemed to have been acknowledged, constitutes full evidence, equivalent to an authentic deed, for the parties who have signed it, their heirs, and their assigns; the provisions of Article 1871 apply to such deeds." Traditionally, signatures are affixed using ink on paper, commonly referred to as wet signatures. However, in the digital era, documents are not limited to conventional physical forms but also exist in digital formats, which may be authenticated using electronic signatures.

Indonesia is currently navigating an era of globalization that significantly influences the advancement of technology and the transformation of business activities. This shift drives business actors toward more effective and efficient practices, most notably through the adoption of e-commerce. Electronic transactions, characterized by their non-face-to-face nature, absence of physical (wet) signatures, and lack of territorial boundaries, enable individuals to engage in transactions across borders through the use of information technology. As technological development progresses, the use of electronic or digital signatures has increasingly replaced conventional (manual) signatures that are typically applied to paper-based agreements. Through electronic media, individuals operate within a virtual environment—an abstract and universal domain that transcends the limitations of physical space and time. (Setiadi, W.T. and Bagiastra, I., 2021).

According to Article 1 Number 12 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, an Electronic Signature is defined as "a signature consisting of Electronic Information that is attached to, associated with, or related to other Electronic Information and which is used as a means of verification and authentication." Fundamentally, a signature serves as a means of validation and functions as a marker of identity within the context of an agreement. In line with technological advancements, conventional (manual) signatures have evolved into electronic signatures, which facilitate the formation of agreements regardless of physical distance. Electronic signatures offer a practical and efficient solution for executing agreements in a timely manner. More broadly, a signature may be interpreted as any

symbol, code, or mark used to legalize a document and signify consent or approval. (Sihombing, L.B, 2020). With regard to the legal standing of electronic signatures in agreements, there exists a fundamental legal basis that governs their enforceability. One such provision is Article 1338 of the Indonesian Civil Code, which states: "All agreements legally made in accordance with the law shall apply as law for the parties who make them." This article affirms the principle of pacta sunt servanda, meaning that contracts—regardless of whether they are executed using conventional or electronic signatures—are binding upon the parties, provided they fulfill the legal requirements.

Electronic signatures utilize technological systems to digitize the process of signing documents. While they offer several advantages—such as convenience, speed, and the ability to facilitate remote transactions—electronic signatures also present certain limitations. One notable drawback is the requirement for specialized software, which is often paid and must be downloaded or installed on a computer or device. This creates accessibility barriers, particularly for individuals or organizations with limited resources or technical proficiency. Moreover, despite the availability of various electronic signature applications, not all users feel secure or confident when conducting transactions that involve signing documents online. Concerns related to data security, authenticity, and the potential for misuse may hinder broader acceptance and trust in electronic signature systems. (Omiyani, S., Suprapto, S. and Saprudin, S., 2023).

The regulatory framework governing Electronic Information and Transactions in Indonesia is primarily established through Law Number 11 of 2008 concerning Electronic Information and Transactions (commonly referred to as the ITE Law). This legislation has undergone several amendments to remain aligned with the rapid advancements in digital technology. The substantial growth in the use of electronic transactions within Indonesian society has prompted lawmakers to develop more comprehensive and systematic legal provisions for the regulation and management of electronic information and transactions. Within this legal context, the ITE Law defines an electronic signature as electronic information that is attached to, associated with, or logically linked to other electronic information, and which serves as a tool for verifying and authenticating identity. (Jessica, P., 2024). This definition suggests that various forms and methods of electronic signatures may be legally recognized, provided they fulfill the essential elements as stipulated by the applicable regulations. Despite the existence of a legal framework that affirms the legitimacy of electronic signatures, their practical implementation continues to encounter several challenges. The adoption rate of electronic signatures in Indonesia remains relatively low. One of the primary issues concerns the certification process and the legal liability of electronic signature providers. These concerns often lead to uncertainty regarding the legal enforceability of electronically signed documents. In practice, the utilization of electronic signatures has not yet reached its optimal potential, particularly due to limitations in technical infrastructure, insufficient public awareness, and the lack of trust in the system's validity and security. (Mayana, R.F. and Santika, T., 2021).

The urgency for further research on electronic signature authentication in online business transactions is becoming increasingly relevant in light of society's growing reliance on digital platforms to conduct economic activities. In practical terms, authentication serves as a critical component in determining the validity and legal legitimacy of an electronic signature. Without a robust and reliable authentication mechanism, the risk of digital identity theft, signature forgery, and legal disputes in online transactions significantly increases. Authentication of electronic signatures is not merely a technical procedure for verifying user identity; it also functions as a legal safeguard that ensures certainty, integrity, and protection for all parties involved in an agreement. Consequently, a comprehensive examination of authentication methods is essential. This includes evaluating cryptographic security standards, the role of digital certification systems (such as Certificate Authorities), and the potential integration with national identity infrastructures. Such an in-depth study is imperative to reinforce the legal validity and public trust in the use of electronic signatures in digital transactions.

Moreover, the proliferation of electronic signature platforms and service providers—many of which implement varying and non-standardized security protocols—poses a risk of systemic vulnerabilities. This lack of uniformity can undermine the overall security and reliability of electronic transactions. In this regard, further research is essential to establish both technical and legal parameters that can serve as national standards. Such parameters would ensure that electronic signature authentication systems operate in accordance with the fundamental principles of integrity, non-repudiation, and legal validity. Given the nature of online business transactions—which are often cross-border and conducted without any physical interaction—there is a critical need for authentication systems that are not only technologically advanced, but also widely accepted by business stakeholders and legal authorities. Therefore, it is imperative to examine issues of system interoperability, cross-jurisdictional recognition, and alignment with international standards. A comprehensive and harmonized approach in these areas will contribute to strengthening trust, legal certainty, and security in digital commercial activities.

Conversely, the low level of digital literacy and limited public trust in the security of digital technologies remain significant challenges that necessitate both policy-driven and education-oriented solutions. Strengthening the legal and technological ecosystem through comprehensive academic research can provide a solid foundation for the formulation of public policies aimed at promoting the broader adoption of validated electronic signatures supported by legitimate and reliable authentication systems. Accordingly, electronic signature authentication in online business transactions should not be viewed solely as a technical concern, but rather as a multidimensional issue that intersects with legal, social, and economic domains.

These aspects must be holistically integrated to ensure the effective and equitable use of electronic signature technologies. Therefore, further scholarly inquiry in this area is crucial to uphold principles of contractual fairness and to enhance transaction security in the digital era.

II. RESEARCH METHOD

This study employs a normative legal research method, which emphasizes a doctrinal approach based on the examination of literature and secondary data in the form of legal materials. The research utilizes two main approaches: the statute approach, which involves the analysis of statutory regulations relevant to the legal issues under investigation; and the conceptual approach, which explores legal concepts and terminologies to construct coherent legal arguments. The sources of legal materials are categorized into three types: primary legal materials, including laws and regulations, official legislative records, and court decisions; secondary legal materials, such as legal textbooks, academic journals, and expert legal opinions; and tertiary legal materials, including legal dictionaries, encyclopedias, and relevant articles from mass media. Data collection techniques are conducted through literature review and case study analysis, while the analytical methods applied are descriptive-analytical and comparative legal interpretation, involving the comparison of relevant legal systems and frameworks. (Djulaeka, and Devi Rahayu., 2020).

III. RESULT AND DISCUSSION

REGULATORY FRAMEWORK AND LEGAL FORCE OF ELECTRONIC SIGNATURES IN ONLINE BUSINESS TRANSACTIONS UNDER INDONESIAN LAW

The advancement of information and communication technology has led to a significant transformation in the business sector, particularly through the emergence and widespread adoption of online transaction mechanisms. Within this digital landscape, the authentication of electronic signatures constitutes a pivotal element in ensuring the security, validity, and legal certainty of electronic agreements. Authentication, in this context, refers to the process of verifying that an electronic signature originates from the purported signatory and that the integrity of the signed document has been maintained since the moment of signing. As such, the regulation of electronic signature authentication in online business transactions is an integral component of a functional and trustworthy digital legal framework. It serves not only as a technical safeguard but also as a legal mechanism to uphold the enforceability and evidentiary value of electronic agreements. (Sumolang, C.G., 2023.).

Normatively, the regulation of electronic signatures in Indonesia has been established under Law Number 11 of 2008 concerning Electronic Information and Transactions (the ITE Law), which has undergone two amendments, the most recent being Law Number 1 of 2024. Article 11 of the ITE Law affirms that electronic signatures possess legal force and are capable of generating legally binding consequences, provided that they fulfill six essential requirements. These requirements include: (1) the electronic signature creation data must be uniquely linked to the signatory; (2) the signature creation data must be under the exclusive control of the signatory at the time of signing; (3) the system used must be capable of detecting any subsequent changes to the electronic signature and the associated electronic information; (4) there must be a mechanism to enable the identification of the signatory; (5) there must be a clear link between the signature and the signed electronic information; and (6) the signatory must give explicit consent to the electronic information being signed. (Lusiana, W., 2024).

Furthermore, the authentication mechanism employed in electronic signatures is fundamentally supported by Public Key Infrastructure (PKI) technology, which operates through the use of a cryptographic key pair: a private key and a public key. The private key is utilized by the signatory to generate a digital signature, whereas the corresponding public key is employed by the recipient or verifier to authenticate the validity of the signature. This cryptographic process is further reinforced by the implementation of a one-way hash function algorithm, which converts the original electronic document into a fixed-length string of characters (the hash value). Any alteration to the document—even a minor change—will result in a completely different hash value, thereby enabling the detection of tampering or unauthorized modifications. As a result, this system ensures both the integrity and authenticity of electronic documents within the context of business transactions, providing a secure and legally reliable means of verification in the digital environment. (Yacub, S.M., Ramadi, R. and Ernawati, D., 2022).

The legal validity of electronic signatures is further reinforced through derivative regulations, particularly Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This regulation categorizes electronic signatures into two types: certified and uncertified. Certified electronic signatures must comply with the requirements governing the use of electronic certificates, which are issued by Electronic Certification Providers (Penyelenggara Sertifikasi Elektronik, or PSrEs) that have been accredited by the Ministry of Communication and Information Technology (Kominfo). Such electronic certificates serve as formal legal validation of both the identity and the authorization of the signatory. In practice, accredited PSrEs—such as PrivyID, VIDA, and PERURI—function as trusted third parties responsible for issuing and managing these certificates, in accordance with security, data integrity, and identity protection standards set forth under the Regulation of the Minister of Communication and Information Technology Number 11 of 2018. Within the framework of Indonesian civil law, the use of electronic signatures aligns with the legal principles established in Articles 1320 and 1338 of the

Indonesian Civil Code. Article 1320 stipulates that a valid agreement must fulfill four essential elements: mutual consent, legal capacity of the parties, a specific object, and a lawful cause. Meanwhile, Article 1338 affirms that all legally executed agreements shall bind the parties with the force of law. Accordingly, as long as these substantive requirements are met, the use of electronic media for contract formation—including the use of electronic signatures as an instrument of agreement—does not diminish the contract's legal validity or enforceability. (Wahyuni, E., Rahman, S. and Risma, A., 2022).

The urgency of authentication in online business transactions lies in its critical role in preventing forgery, identity theft, and repudiation by parties to a digital contract. As such, authentication mechanisms must not only verify the authenticity of the signatory's identity but also ensure the integrity of the electronic document and provide a reliable basis for non-repudiation. These three elements—authenticity, integrity, and non-repudiation—constitute fundamental principles in information security architecture, particularly in the context of electronic transactions that are transnational and occur without physical interaction. Ensuring these principles is essential to maintaining trust, legal certainty, and the enforceability of digital agreements in the increasingly borderless and intangible nature of modern commercial exchanges. (Listiyani, N., 2022). Within the procedural legal framework, the validity of electronic signatures as legitimate legal evidence has been explicitly recognized under Article 5 paragraph (2) of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). This provision is further strengthened by Article 49 paragraph (3) of Government Regulation Number 80 of 2019 concerning Trade through Electronic Systems, which affirms that proof of transactions using certified electronic signatures may be considered as authentic written evidence (authentic deed). Accordingly, the authentication of electronic signatures serves a dual function: first, as a mechanism to preserve the integrity of digital contracts; and second, as a legal safeguard that ensures protection for the parties engaged in online transactions. This recognition reinforces the enforceability of electronic agreements within the Indonesian legal system and supports the broader development of secure and reliable digital commerce. (Nafri, M., 2019).

Based on the foregoing analysis, the regulatory framework governing electronic signature authentication in online business transactions in Indonesia rests on a relatively robust legal foundation. Nevertheless, the effectiveness of its implementation remains contingent upon the synergistic integration of regulatory frameworks, technological advancements, and public legal awareness. To foster a secure, legally compliant, and trustworthy electronic transaction ecosystem, it is imperative to undertake comprehensive public education initiatives, enhance the national digital security infrastructure, and ensure consistent regulatory oversight of accredited certification authorities. Only through such coordinated efforts can the authentication of electronic signatures fulfill its intended function as a pillar of legal certainty and protection in the digital economy.

In the realm of electronic transactions, the regulation of electronic signature authentication is inextricably linked to the element of legal force attributed to the signature. Authentication functions as the primary mechanism for verifying that an electronic signature has been created by, and is legally associated with, the purported signatory. Legal force, on the other hand, affirms that such a signature may serve as the basis for valid legal evidence in commercial transactions. Accordingly, a direct and interdependent relationship exists between authentication and legal force: proper authentication constitutes a necessary condition for an electronic signature to attain legal validity and evidentiary recognition before the law. The regulation of authentication, as codified in Article 11 of Law Number 1 of 2024 on Amendments to the Law on Electronic Information and Transactions, is therefore not merely technical in nature but also normative, as it pertains directly to the legal enforceability of electronically signed instruments. In this context, the validity of an electronic signature cannot be assessed solely by its digital format or the act of affixing it, but must also consider the robustness and legitimacy of the authentication procedures employed. It is through this authentication process that the electronic signature derives its legal authority and evidentiary weight. Hence, any legal discourse on authentication must be simultaneously framed as a discussion on legal force, as both elements are mutually reinforcing and together constitute a coherent legal framework essential to ensuring legal certainty in online business transactions.

The emergence of electronic signatures in the era of digital transformation has become a pivotal legal instrument in ensuring the validity and enforceability of online business transactions. In tandem with the accelerated advancement of information and communication technologies, the demand for efficiency and promptness in contract formation and transactional processes has driven the digitization of document authentication mechanisms—most notably through the utilization of electronic signatures (Tanda Tangan Elektronik or TTE). Within the Indonesian legal framework, the legal force of electronic signatures has attained clear statutory recognition through Law Number 1 of 2024, which serves as the second amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Article 11 of the ITE Law affirms that electronic signatures shall possess legal force and binding legal consequences, provided that they fulfill a set of statutory requirements. These requirements include, inter alia, the verifiable authenticity of the signatory's identity and the assurance of the integrity and unaltered condition of the electronically signed document.

Normatively, the legal force of an electronic signature does not merely derive from its function as a symbol of digital consent, but is intrinsically linked to the authentication and identity verification mechanisms that underpin its use. This authentication process is governed by Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions, as well as by the Regulation of the Minister of Communication and Information Technology Number 11 of 2018 concerning the Implementation of Electronic Certification. Pursuant to these regulations, a legally valid electronic signature

must be supported by an Electronic Certificate issued by an accredited Electronic Certification Provider (Penyelenggara Sertifikasi Elektronik, or PSrE) recognized by the government, such as PrivyID, VIDA, and PERURI (Wahyuni, E., Rahman, S., & Risma, A., 2022). The electronic certificate serves as a digital instrument containing verified legal identity information of the transacting parties. This enables the assurance of data integrity, identity authentication, and the fulfillment of the principle of non-repudiation—namely, the legal impossibility for the signatory to deny authorship or approval of the signed document.

In practical application, certified electronic signatures are increasingly utilized in a wide range of transactions, particularly those involving financial institutions, fintech service providers, public administration, and commercial agreements executed through digital platforms. The Electronic Information and Transactions Law (ITE Law) not only acknowledges the legitimacy of electronic signatures as instruments of legal authentication, but also affirms that electronic information and/or its printouts may be admissible as legal evidence, as stipulated in Article 5 paragraph (2) of the ITE Law (Susilowati, D.E., Muhtarom, M., & Junaidi, A., 2025). This provision signifies a progressive expansion of Indonesia's procedural evidentiary framework, which has traditionally been limited to physical documentation and handwritten signatures. Within the context of civil law, the evidentiary function of an electronic signature (Tanda Tangan Elektronik or TTE) may therefore be equated with that of a private deed (akta di bawah tangan), as provided for in Article 1875 of the Indonesian Civil Code, provided that the electronic signature is acknowledged by the parties and satisfies the essential elements of a valid agreement as set forth in Article 1320 of the Civil Code.

In addition to the aspects of validity and evidentiary strength, the legal framework also provides both preventive and repressive legal protection for parties involved in the use of electronic signatures. Preventive legal protection is manifested through statutory provisions that establish normative guidelines for the implementation of electronic signatures—among them, the obligation of Electronic Certification Providers (Electronic Certification Providers, or PSrE) to safeguard the integrity and confidentiality of user data, as well as the imposition of technical and legal requirements for the issuance of electronic certificates. Conversely, repressive legal protection is reflected in the imposition of criminal sanctions for the misuse or forgery of electronic signatures. Such violations are regulated under Article 35 in conjunction with Article 51 paragraph (1) of the Electronic Information and Transactions Law (ITE Law), which provides for penalties of up to twelve (12) years of imprisonment and/or a maximum fine of twelve billion Indonesian Rupiah (IDR 12,000,000,000). These stringent sanctions underscore the seriousness with which the law treats the integrity of electronic systems, reflecting the importance of electronic signatures in maintaining legal certainty and fostering public trust in digital transactions.

Electronic signatures in online business transactions are not merely digital representations of agreements, but are legally recognized instruments that have enforceable legal consequences. As stipulated in various regulatory frameworks—especially Government Regulation Number 82 of 2012, the substantive provisions of which have been integrated into Government Regulation Number 71 of 2019—and further strengthened by the principles of contract law, electronic signatures are given the same legal standing as handwritten (wet) signatures with regard to the validity of the agreement and its binding effect on the parties. Thus, transactional documents executed using electronic signatures, provided they meet the required legal formalities and procedural standards, can be accepted as authentic written evidence, including in court proceedings. Thus, the regulation of the legal force of electronic signatures in online business transactions reflects the Indonesian legal system's commitment to adapting to the evolving digital landscape through a responsive and progressive legislative framework. Comprehensive regulatory provisions, when supported by robust authentication technologies and heightened public legal awareness, serve to foster a secure, reliable, and legally certain digital transaction ecosystem. In this regard, electronic signatures are not merely instruments of administrative efficiency, but have emerged as fundamental components of the legal infrastructure that underpins commerce in the digital era.

IV. CONCLUSION

Electronic signatures have attained unequivocal legal recognition and enforceability within Indonesia's digital legal regime, particularly through Article 11 of Law Number 1 of 2024 amending the ITE Law. Their legal force is predicated on compliance with specific authentication criteria—ensuring identity integrity, exclusive control, non-alteration, and express consent—while their technological validity is secured through the deployment of Public Key Infrastructure (PKI), hash algorithms, and accredited electronic certificates issued by PSrEs under Kominfo's authority. These instruments operate not only as tools of digital consent but as legally binding mechanisms equivalent to conventional signatures under the Civil Code, insofar as they fulfill the fundamental elements of a valid contract.

In evidentiary terms, Articles 5(2) of the ITE Law and 49(3) of GR 80/2019 elevate certified electronic signatures to the level of authentic written evidence, thereby integrating them into formal legal proceedings. Indonesia's regulatory framework further ensures legal protection through a dual approach: preventive safeguards via normative and technical standards, and repressive sanctions for electronic signature misuse under Article 51 of the ITE Law. Thus, electronic signatures are not merely procedural conveniences but integral to the enforceability, probative value, and legal certainty of online business transactions.

Strengthening digital legal literacy and institutional oversight remains essential to consolidating a robust, secure, and trusted e-commerce legal ecosystem.

REFERENCES

1) Djulaeka, and Devi Rahayu., 2020. Buku Ajar: Metode Penelitian Hukum. Scopindo Media Pustaka.
2) Jessica, P., 2024. Cyber Notary dan Digitalisasi Tanda Tangan. Deepublish.
3) Listiyani, N., 2022. Analisis Yuridis Pelaksanaan Cyber Notary di Indonesia di Kaitkan Dengan Kewajiban Para Pihak Untuk Menandatangani Akta Secara Elektronik (Master's thesis, Universitas Islam Sultan Agung (Indonesia)).
4) Mayana, R.F. and Santika, T., 2021. Legalitas tanda tangan elektronik: posibilitas dan tantangan notary digitalization di Indonesia. ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan, 4(2).
5) Nafri, M., 2019. Dokumen Elektronik Sebagai Alat Bukti Dalam Hukum Acara Perdata di Indonesia. Maleo Law Journal, 3(1).
6) Omiyani, S., Suprapto, S. and Saprudin, S., 2023. Digitalisasi Tandatangan Elektronik pada Akta Notaris. JIM: Jurnal Ilmiah Mahasiswa Pendidikan Sejarah, 8(4).
7) Setiadi, W.T. and Bagiastra, I., 2021. Keabsahan Tanda Tangan Pada Akta Autentik Secara Elektronik Ditinjau Dari Cyber Notary (Doctoral dissertation, Udayana University).
8) Sihombing, L.B., 2020. Keabsahan tanda tangan elektronik dalam akta notaris. Jurnal Education and development, 8(1).
9) Sumolang, C.G., 2023. Sanksi Hukum Bagi Pemalsuan Tanda Tangan Elektronik Menurut Undang-Undang Tentang Informasi Dan Transaksi Elektronik. Lex Privatum, 12(3).
10) Susilowati, D.E., Muhtarom, M. and Junaidi, A., 2025. Analisis Yuridis Keabsahan Tanda Tangan Digital dalam Transaksi E-Commerce di Indonesia. JURNAL PENELITIAN SERAMBI HUKUM, 18(01).
11) Wahyuni, E., Rahman, S. and Risma, A., 2022. Keabsahan Digital Signature/Tanda tangan Elektronik Dinjau Dalam Perspektif Hukum Perdata dan UU ITE. Journal of Lex Generalis (JLG), 3(5).
12) Yacub, S.M., Ramadi, R. and Ernawati, D., 2022. Public Key Infrastructure: Kerangka Validasi Yang Disempurnakan. Jurnal Tiple A Pendidikan Teknologi Informasi dan Teknologi Informasi, 1(2).