KAMPUS AKADEMIK PUBLISING
Jurnal Sains Student Research
Vol.1, No.1 Oktober 2023
e-ISSN: 3025-9851; p-ISSN: 3025-986X, Hal 752-762
DOI: https://doi.org/10.61722/jssr.v1i2.394

Kekuatan Hukum dan Aspek Keamanan Dalam Tanda Tangan Elektronik

Triana Wati
Universitas Trunojoyo Madura
Alamat: Jl.Raya Telang, PO,Box. 2 Kamal-Madura
Korespondensi penulis : trianawati173@gmail.com

Abstract. *An Electronic Signature is an electronically generated signature used for authentication and verification of electronic documents. Electronic Signature has the potential to replace wet signatures in a variety of transactions, including contracts, agreements, and other legal documents. Electronic Signature is regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions. Article 11 of the Electronic Signature Law states that Electronic Signature has legal force and legal consequences that are valid and binding as long as it meets certain requirements. The security aspect is also an important consideration in the use of Electronic Signature. Electronic Signature must be guaranteed authenticity and integrity so that it cannot be falsified or altered. This journal discusses the legal strength and security aspects of Electronic Signature. This journal aims to provide a better understanding of Electronic Signature and how Electronic Signature can be used safely and effectively in various transactions*

Keywords: *Electronic Signature, Legal Strength, Security Aspect.*

Abstrak. Tanda Tangan Elektronik (TTE) adalah tanda tangan yang dibuat secara elektronik yang digunakan untuk otentifikasi dan verifikasi dokumen elektronik. Tanda tangan elektronik memiliki potensi untuk menggantikan tanda tangan basah dalam berbagai transaksi, termasuk kontrak, perjanjian, dan dokumen hukum lainnya. Tanda tangan elektronik diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 11 UU ITE menyatakan bahwa tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah dan mengikat sepanjang memenuhi persyaratan tertentu. Aspek keamanan juga menjadi pertimbangan penting dalam penggunaan tanda tangan elektronik. Tanda tangan elektronik harus dapat dijamin keaslian dan integritasnya agar tidak dapat dipalsukan atau diubah. Jurnal ini membahas kekuatan hukum dan aspek keamanan tanda tangan elektronik. Jurnal ini bertujuan untuk memberikan pemahaman yang lebih baik tentang tanda tangan elektronik dan bagaimana tanda tangan elektronik dapat digunakan secara aman dan efektif dalam berbagai transaksi.

Kata kunci: Tanda tangan elektronik, kekuatan hukum, aspek hukum.

Received Agustus 30, 2023; Revised September 2, 2023; Oktober 23, 2023
* Triana Wati, rianawati173@gmail.com

PENDAHULUAN

Tanda tangan basah merupakan tanda tangan yang dibuat secara manual pada dokumen fisik. Tanda tangan basah telah menjadi bagian penting dari kehidupan kita sehari-hari, mulai dari dokumen pribadi hingga dokumen hukum. Namun, seiring dengan perkembangan teknologi, tanda tangan basah mulai bergeser ke tanda tangan elektronik.

Tanda Tangan Elektronik telah menjadi salah satu inovasi penting dalam dunia digital saat ini. Dalam era dimana transaksi online semakin umum, tanda tangan elektronik memainkan peran krusial dalam memvalidasi dan mengamankan dokumen elektronik. Tanda tangan elektronik memungkinkan individu dan orgaisasi untuk melakukan transaksi secara efisien, cepat, dan aman tanpa perlu bertatap muka secara fisik.[1]

Namun, penggunaan tanda tangan elektronik juga memunculkan beberapa pertanyaan hukum dan keamanan yang perlu dipertimbangkan. Dalam konteks ini, penting untuk memahami kekuatan hukum dari tanda tangan elektronik serta aspek keamanan yang terkait dengannya. Sebagai alat untuk menggatikan tanda tangan basah, tanda tangan elektronik harus memiliki kekuatan hukum yang setara dengan tanda tangan konvensional. Selain itu, keamanan tanda tangan elektronik juga mejadi pertimbangan penting dalam memastikan integritas dan keabsahan dokumen elektronik.

Penulisan ini bertujuan untuk mengetahui kekuatan hukum dan aspek keamanan tanda tangan elektronik. Melalui tinjauan literatur, penulisan ini akan menggali landasan hukum yang mengatur penggunaan tanda tangan elektronik serta mengalisis kerangka kemanan yang diterapkan untuk melindungi tanda tangan elektronik dari penyalahgunaan dan pemalsuan.

Hasil dari penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam tentang kekuatan hukum dan aspek keamanan tanda tangan elektronik. Penulisan ini juga dapat memberikan panduan untuk dapat mengembangkan kebijakan dan sistem yang lebih baik untuk mengatur dan melindungi penggunaan tanda tangan elektronik.

---

[1] (Mayasari, 2022)

METODE PENELITIAN

Penelitian ini adalah penelitian hukum yuridis normativ. Metode ini dilakukan dengan cara meneliti bahan Pustaka hukum yang ada. Penelitian yuridis normativ membahas doktrin-doktrin atau asas ilmu hukum serta peaturan perundang-undangan dalam hal yang berkaitan dengan kedudukan hukum tanda tangan elektronik dalam perkembangan era digital ini.[2]

Bahan hukum yang digunakan dalam penulisan ini yaitu bahan hukum primer terdiri dari peraturan perundang-undangan. Bahan hukum sekunder terdiri dari buku teks, jurnal hukum, kamus hukum, hasil penelitian hukum, serta dokumen penunjang lainnya.

PEMBAHASAN

A. Kekuatan Hukum Tanda Tangan Elektronik

Tanda tangan elektronik adalah data elektronik yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik lainya yang digunakan sebagai alat verifikasi dan autentifikasi.[3] Sederhananya, tanda tangan elektronik merupakan pengganti digital dari tanda tangan basah yang digunakan untuk menandatangani dokumen eletronik. Tanda tangan elektronik memiliki berbagai kegunaan, diantaranya:

1. Mempercepat proses penandatanganan dokumen. Dokumen elektronik dapat ditandatangani secara digital dari mana saja, kapan saja, tanpa harus bertemu langsung dengan pihak lain.
2. Meningkatkan keamanan dan integritas dokumen. Tanda tangan elektronik dilengkapi dengan fitur keamanan yang dapat mencegah pemalsuan dan manipulasi dokumen.
3. Menghemat biaya dan waktu. Tanda tangan elektronik dapat menghemat biaya kertas, tinta, dan pengiriman.
4. Meningkatkan produktivitas dan efisiensi. Tanda tangan elektronik dapat mempercepat proses bisnis dan alur kerja.

[2] (Ali, 2013)
[3] (Ponorogo, 2019)

5. Mempermudah transaksi elektronik. Tanda tangan elektronik dapat digunakan untuk menandatangai berbagai jenis dokumen elektronik, seperti kontrak, perjanjian dan faktur.

Dasar hukum tanda tangan elektronik di Indonesia diatur dalam UU no 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 11 UU ITE menyatakan bahwa Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah dan mengikat sepanjang memenuhi persyaratan, yaitu:[4]

1. TTE dibuat oleh penandatangan yang sah
2. TTE dibuat degan menggunakan perangkat luak yang memenuhi persyaratan tertentu
3. TTE dapat diverifikasi dengan meggunakan perangkat lunak yang memenuhi persyaratan tertentu
4. TTE dapat diidentifikasi dengan penandatangannya

Pasal 11 UU ITE tersebut merupakan pegangan hukum yang kuat terhadap tanda tangan elektronik. Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sama dengan tanda tangan basah. Hal ini berarti bahwa Tanda tangan elektronik dapat digunakan sebagai alat bukti yang sah dan dapat dipertanggungjawabkan di Pengadilan. Selain UU ITE dasar hukum Tanda tangan elektronik juga diatur dalam Peraturan Perundang-Undangan lainya, antara lain:

1. Peraturan pemerintah No. 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)
2. Peraturan Menteri Komunikasi dan Informatika Nomor 26 tahun 2016 tentang Penyelenggara Sertifikasi Elektronik (Permen Kominfo 26/2016)
3. Peraturan Menteri Komunikasi dan Informatika Nomor 5 tahun 2017 tentang Penyelenggaraan Sertifikasi Sertifikasi Elektronik (Permen Kominfo 5/2017)

PP PSTE mengatur tentang penyelenggaraan sistem dan transaksi elektronik, termasuk tanda tangan elektronik[5]. Permen Kominfo 26/2016 mengatur tentang penyelenggaraan sertifikasi elektronik, yang merupakan salah satu komponen penting dalam tanda tangan elektronik. Permen Kominfo 5/2017 mengatur tetang perubahan

[4] UU 11 Tahun 2008
[5] (laumuri & dkk, 2014)

atas Permen Kominfo 6/2016. Beberapa putusan pengadilan dan kasus hukum telah menjadi poin kritis yang memengaruhi pandangan terhadap kekuatan hukum tanda tangan elektronik menciptakan landasan hukum yang berkembang baik di Indonesia maupun diluar negri. Kasus-kasus ini mencerminkan evolusi dan penerimaan tanda tangan elektronik dalam lingkungan hukum, memberikan petunjuk yang berharga tetang bagaimana yuridiksi tertentu menangani dan mengakui validitas tanda tangan elektronik. Contoh kasus yang mencolok antara lain:

Di Indonesia, salah satu putusan pengadilan yang berpengaruh adalah Putusan Mahkamah Agung Nomor 313 K/Pdt.Sus-PTUN/2015. Dalam putusan tersebut, Mahkamah Agug menyatakan bahwa Tanda tangan elektronik yang dibuat dengan menggunakan sertifikat elektronik yang telah terdaftar di Badan Siber dan Sandi Negara (BSSN) memiliki kekuatan hukum yang sama dengan tanda tangan basah. Putusan ini juga telah mendorong adopsi tanda tangan elektronik di berbagai sektor, termasuk sektor pemeritahan, bisnis, dan Pendidikan.

Di luar negri, salah satu kasus hukum yang berpengaruh adalah kasus Citibank vs. Signature Financial Group,Inc. yang terjadi di Amerika Serikat. Dalam kasus tersebut, pengadilan menyatakan bahwa Tanda tangan elektronik yang dibuat dengan mengguakan sertifikat elektronik yag terdaftar di VeriSign memiliki kekuatan hukum yang sama dengan tanda tangan basah.

Putusan ini penting karena telah memberikan pengakuan hukum terhadap tanda tangan elektronik di Amerika Serikat. Putusan ini juga telah mendorong adopsi tanda tangan elektronik di berbagai negara di dunia, termasuk Indonesia. Dimana kasus hukum tersebut telah menunjukkan bahwa tanda tangan elektronik memiliki kekuatan hukum yang sama dengan tanda tangan basah. Hal ini telah mendorong adopsi tanda tangan elektronik secara luas di berbagai negara di dunia.

Melalui analisis mendalam terhadap putusan-putusan tersebut, dapat dilihat pergeseran pandangan hukum yang semakin mendukung dan mengakui keberlakukan tanda tangan elektronik sebagai alat sah dalam transaksi bisnis dan hukum. Oleh karena itu, pemahaman mendalam terhadap kasus-kasus ini menjadi esensial dalam merancang regulasi dan kebijakan yang memadai seiring dengan terus berkembanganya teknologi tanda tangan elektronik.

B. Aspek Keamanan Tanda Tangan Elektronik

Tanda tangan elektroik memiliki potensi besar untuk menggantikan peran tanda tangan basah dalam berbagai transaksi, membawa kemudahan dan efisiensi dalam dunia digital. Namun, seiring dengan keuntungan tersebut, perlu diakui bahwa tanda tangan elektronik juga membawa potensi acaman terhadap integritas dan keamanan. Konsep integritas dalam konteks tanda tangan elektronik mencakup perlidungan terhadap segala bentuk perubahan yang dapat terjadi setelah tanda tangan tersebut dibuat.[6]

Potensi ancaman terhadap integritas tanda tangan elektronik membuka ruang bagi berbagai tantangan yang perlu diatasi dengan cermat. Beberapa di antaranya mencakup risiko perubahan data yang tidak sah setelah proses tanda tangan, yang dapat merugikan keaslian dokumen atau informasi yang ditandatangani. Oleh karena itu, menjaga integritas tanda tangan elektronik menjadi krusial utuk memastikan bahwa dokumen atau data yang ditandatangani tetap utuh dan tidak terpengaruh oleh manipulasi yang tidak diinginkan.

Ancaman terhadap integritas tanda tangan elektronik tidak hanya berkaitan dengan potensi perubahan data, tetapi juga melibatkan risiko penggunaan tanda tangan tersebut dalam konteks yang tidak sah atau untuk tujuan yang tidak diinginkan. Oleh karena itu, perlindungan terhadap integritas tanda tangan elektronik harus mencakup lagkah-langkah yang dapat memastikan bahwa tanda tangan tersebut tidak dapat disalahgunakan atau dimanfaatkan oleh pihak yang tidak berwenang. Potensi ancaman terhadap integritas dan keamanan tanda tangan elektronik meliputi:

1. Pemalsuan Tanda Tangan Elektronik

Pemalsuan tanda tangan elektronik dapat dilakukan dengan cara mengganti data dalam tanda tangan elektronik, misalnya dengan mengganti data penandatanganan atau data dokumen yang ditandatangani.

2. Intervensi Terhadap Dokumen yang Ditandatangani

Intervensi terhadap dokumen yang ditandatangani dapat dilakukan dengan cara mengubah data dalam dokumen setelah ditandatangani.

---

[6] (Patriato, 2008)

3. Pencurian Kunci Privat

Kunci privat adalah kunci yang digunakan untuk membuat tanda tangan elektronik. Kunci privat harus bersifat rahasia dan tidak boleh dibagikan kepada siapapun. Jika kunci privat dicuri, maka yang mencuri kunci privat dapat membuat tanda tangan elektronik palsu.

4. Kebocoran Data Privat

Data pribadi, seperti nama, Alamat dan nomor identitas yang digunakan untuk membuat tanda tangan elektronik dapat disalahgunakan oleh pihak yang tidak bertanggung jawab.

Dari berbagai macam potensi ancaman terhadap integritas dan keamanan tanda tangan elektronik beberapa aspek keamanan diterapkan untuk memastikan integritas otentikasi dan kerahasiaan tanda tangan elektronik. Berikut penjelasan mengenai aspek keamanan tersebut:[7]

1. Enkripsi Kuat

Penggunaan algoritma enkripsi yang kuat untuk melindungi data dari tanda tangan elektronik dari akses yang tidak sah atau perubahan yang tidak sah dengan penggunaan algoritma yang benar dapat mencegah pembacaan atau modifikasi oleh pihak yang tidak berwenang dan memberikan Tingkat keamanan tambahan

2. Otentikasi Pengguna

Penerapan metode otentikasi yang kuat seperti kata sandi verifikasi dua faktor atau biometric untuk memastikan identitas pengguna yang sah yang bertujuan untuk meminimalisir risiko penggunaan tanda tangan oleh pihak yang tidak berwenang atau pihak dengan identitas palsu.

3. Integritas Data

Integritas data dalam konteks tanda tangan elektronik merujuk pada keadaan dimana data yang ditandatangani tetap utuh dan tidak mengalami perubahan yang tidak sah. Untuk mencapai integritas teknik Hash atau Checkshum perlu digunakan. Hash adalah fungsi matematis yang menghasilkan nilai unik berdasarkan input data. Checkshum

[7] (Mohammad, 2016)

adalah nilai numerik yang dihasilkan dari data dan digunakan untuk memeriksa kesalahan. Dengan menerapkan integritas data menggunakan teknik Hash atau Checkshum tanda tangan elektronik dapat diandalkan untuk memastikan bahwa informasi yang ditandatangani tetap utuh dan tidak dapat dimanipulasi secara tidak sah oleh pihak yang tidak berwenang.

4. Penyimpana yang Aman

Menyimpan tanda tangan elektronik dan dokumen secara aman merupakan hal dasar untuk menghindari ancaman keamaan dalam digital dengan menggunakan protokol penyimpanan yang sesuai yang akan melindungi data dari akses yang tidak sah atau kebocoran yang dapat membahayakan keamanan informasi.

5. Pemantauan Aktivitas

Dalam konteks tanda tangan elektronik merujuk pada praktik mencatat secara rinci setiap aktivitas yang terkait dengan pembuatan, verifikasi, atau pengelolaan tanda tangan elektronik. Hal ini melibatkan pembuatan catatan yang merinci tentang setiap langkah yang diambil oleh pengguna, sistem, atau entitas terkait sepanjang siklus hidup tanda tangan elektronik. Informasi yang direkam meliputi waktu, lokasi, pengguna yang terlibat, dan jenis aktivitas yang dilakukan. Dengan menerapkan audit dan rekam jejak, organisasi dapat meningkatkan resposibilitas dan keandalan tanda tangan elektronik, serta memperkuat kapabilitas mereka untuk menghadapi dan merespon potensi ancaman keamanan dengan cepat dan efisien.

6. Kebijakan Akses dan Izin

Menetapkan kebijakan yang jelas terkait dengan hak akses dan izin untuk penggunaan tanda tangan elektronik. Yang bermanfaat mengontrol dan membatasi akses hanya kepada pihak yang berwenang mencegah penggunaan yang tidak sah

7. Tanda Tangan Digital

Menggunakan tanda tangan digital untuk memvalidasi otentikasi dan integritas tanda tangan dengan tujuan untuk memberikan bukti keaslian dan keintegritasan tanda tangan elektronik, meningkatkan Tingkat kepercayaan

8. Audit dan Rekam Jejak

Merekam aktivitas terkait tanda tangan elektronik untuk keperluan audit dan investigasi yang bermanfaat untuk memfasilitasi pelacakan, analisis, dan perbaikan setelah terjadi insiden keamanan.

Dengan melakukan penyelarasan yang cermat dan holistik terhadap semua aspek keamanan yang terlibat, tanda tangan elektronik tidak hanya mejadi sekadar tanda tangan digital, melainkan menjadi suatu alat yang memancarkan keamanan tingkat tinggi dan dapat diandalkan sepenuhnya dalam memfasilitasi berbagai transaksi digital. Peyelarasan ini melibatkan implementasi langkah-langkah keamanan yang menyeluruh, termasuk penggunaan enkripsi yang kuat, metode otentikasi yang canggih dan praktik pengelolaan integritas data.

Dengan merancang kebijakan penyimpanan yang aman dan melibatkan pemantauan aktif atas aktivitas terkait, tanda tangan elektronik tidak hanya menjamin keutuhan data yang ditandatangani tetapi juga memberikan kepercayaan yang kuat terkait dengan keaslian dan keamanan informasi. Melalui penggunaan tanda tangan digital yang didukung oleh sertifikat digital, proses validasi otentikasi dan integritas semakin ditingkatkan, memberikan kepastian tambahan terhadap keandalan tanda tangan elektronik.

Kebijakan akses dan izin yang terdefinisi dengan jelas juga menjadi bagian integral dari upaya penyelarasan ini, memastikan bahwa hanya pihak yang berwenang yang memiliki hak akses untuk membuat, mengakses, atau mengelola tanda tangan elektronik. Sementara itu, rekam jejak dan sistem audit yag efektif memainkan peran penting dalam membantu mendeteksi dan menanggapi potensi ancaman keamanan, memungkinkan langkah-langkah perbaikan yang cepat dan efisien.

Secara keseluruhan, dengan menyelaraskan semua aspek keamanan ini, tanda tangan elektronik bukan hanya sekadar sarana transaksi digital, tetapi mejadi pilar keamanan yang kokoh dalam ekosistem digital, memberikan kepastian dari kepercayaan yang diperlukan dalam era yang terus berkembang ini.

Penerapan tanda tangan elektronik, sebagai langkah transformasional dalam dunia bisnis dan administrasi, memang membawa sejumlah manfaat signifikan dalam mengoptimalkan proses transaksi dan mendigitalkan dokumen. Kecepatan, efisiensi, dan kemudahan akses yang diberikan oleh tanda tangan elektronik telah mengubah cara

banyak organisasi berinteraksi dan beroperasi. Meskipu begitu, perlu diakui bahwa peralihan ke tanda tangan elektronik juga membawa sejumlah kendala dan tantangan yang perlu diatasi agar penerapannya berjalan dengan lancar dan dapat diterima secara luas.

1. Kendala Teknis

a. Ketersediaan Infrastruktur

Tanda tangan eektronik membutuhkan infrastruktur pendukung, seperti perangkat keras dan perangkat lunak. Ketersediaan infrastruktur pendukung yang memadai menjadi salah satu kendala utama dalam penerapan tanda tangan elektronik.

b. keamanan

Tanda tangan elektronik harus memiliki Tingkat keamanan yang tinggi untuk mencegah pemalsuan dan penyalahgunaan. Pengembangan teknologi tanda tangan elektronik yang lebih aman dan andal perlu dilakukan untuk mengatasi kendala ini.

c. Kompatibilitas

Tanda tanga elektroik harus dapat digunakan secara lintas platform dan lintas aplikasi. Pembangunan standar tanda tangan elektronik yang bersifat terbuka dan interoperable perlu dilakukan unuk mengatasi kendala ini.

2. Kendala Non-Teknis

a. Kesadaran Masyarakat

Masyarakat masih belum sepenuhnya memahami manfaat dan keamanan tanda tangan elektroik. Edukasi dan sosialisasi yang lebih luas perlu dilakukan untuk meingkatkan kesadaran masyarakat tentang tanda tangan elektronik.

b. Kebijakan dan Regulasi

Kebijakan dan regulasi yang mengatur tanda tangan elektronik masih perlu disempurnakan. Kebijakan dan regulasi yang jelas dan konsisten akan mendorong adopsi tanda tangan elektronik secara luas.

Menghadapi kendala kendala ini memerlukan keterlibatan aktif dari pihak swasta, pemerintah dan lembaga keamanan siber untuk memastikan bahwa penerapan tanda tangan elektronik berjalan dengan lancar, efektif dan dapat diterima oleh semua pihak

yang terlibat. Dengan mengatasi kendala ini potensi penuh tanda tangan elektronik sebagai alat yang efisien dan handal dapat sepenuhnya diwujudkan.

KESIMPULAN DAN SARAN

Tanda tangan elektronik diakui memiliki kekuatan hukum yang setara dengan tanda tangan basah, dasar hukum tanda tangan elektronik terdapat dalam UU ITE Nomor 11 Tahun 2008 dan PERPU terkait. Potensi ancaman terhadap integritas tanda tangan elektronik mencakup pemalsuan, intervensi dokumen, pencurian dan kebocoran data pribadi sedangkan langkah keamanan yang dapat diambil yaitu melibatkan enkripsi kuat, otentikasi penggunan, integritas data, penyimpanan aman, pemantauan aktivitas, kebijakan akses, dan tanda tangan digital. Tanda tangan elektronik memberikan manfaat seperti percepatan proses, keamanan dokumen, efisiensi, dan kemudahan transaksi elektronik. Selain memberikan kemanfaatan tentunya tanda tangan elektronik masih memiliki kendala baik dalam bidang teknis maupun non teknis.

DAFTAR PUSTAKA

Buku

Zainuddin Ali. (2013). *Metode Penelitian Hukum.* Jakarta: Sinar Grafika

Patriato, J. (2008). *Dengan Berlakunya Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Tanda Tangan Elektronik.*

Artikel Jurnal, Website

Ariadi, I. W. (2016). Bentuk-Bentuk Digital Signature yang Sah Dalam Transaksi Elektronikdi Indonesia. *vol.5*.

Christi, N. M; Maria Margaretha; Ari Yuliartini Griadhi, Ni Made (2014). Keabsahan Tanda Tangan Elektronik. *Kertha Senaya*.

Mayasari, Y. (2022). Kedudukan Hukum Tada Tangan Elektronik. *Jurnal Teknologi Informasi* .

Mohammad, I. (2016). Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma RSA. *CESS (Jurnal of Computer Engineering System And Sains)*.

Ponorogo, D. K. (2019, September 19). *Tanda Tangan Elektronik vs Tanda Tangan Digita*. Retrieved from Dinas Komunikasi Informatika Dan Statistik Kabupaten Ponorogo: https://kominfo.ponorogo.go.id/tanda-tangan-elektronik-vs-tanda-tangan-digital/ diakses pada tanggal 16 November 2023 pukul 18.16

R, S. (2018). Keabsahan Digital Signature dalam Perjajian E-Commerce. *Jurnal of Law*.

Tandiabang, R. M. (n.d.). Otentikasi Dokumen Elektronik Meggunakan Tanda Tangan Digital. *artikel jurnal ilmiah*.

Peraturan Perundang-undangan

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik