

Urgensi *Trusted Third Party* Sebagai Acuan Autentifikasi Tanda Tangan Digital Dalam Pembuatan Akta Notaris

¹Muhammad Fernando, ²Abdul Salam

^{1,2}Magister Kenotariatan Fakultas Hukum Universitas Indonesia

Email: muhamadfernandoo@gmail.com

Article Info	Abstract
<p>Article history: Received : 16 Desember 2022 Publish : 14 Januari 2023</p>	<p><i>This study examines Legal vacuum issue about trusted third party Who is authorized to judge the authentication of digital signature. That related to a profession the notary in executing function of his term of office This study aims to analyse and to established the ideal regulations about trusted third party. This research is a Normative research, with a conceptual approach, statute approach. The results of this study is Indonesia needed to formulate regulation about trusted third party, for maintaining the Legal certainty to society Who runs the economic activities and also a Notary Which carries on the function of his term of office.</i></p>
<p>Keywords: <i>Digital Signature, Notary, trusted third party</i></p>	

Article Info	Abstrak
<p>Article history: Received : 16 Desember 2022 Publish : 14 Januari 2023</p>	<p>Penelitian ini meneliti kekosongan hukum mengenai Notaris yang berwenang melakukan verifikasi tanda tangan digital, yang berhubungan profesi notaris dalam menjalani fungsi jabatannya. Tujuan dari penelitian ini adalah untuk menganalisis dan menawarkan konsep ideal mengenai norma yang mengatur kewenangan Notaris sebagai pihak ketiga dalam menilai autentifikasi sebuah tanda tangan digital Penelitian hukum ini adalah penelitian yang bersifat normatif dengan menggunakan pendekatan perundang-undangan dan pendekatan konseptual. Hasil dari penelitian ini adalah, perlunya diatur dalam hukum positif di Indonesia mengenai pihak resmi yang berwenang untuk menilai autentifikasi sebuah tanda tangan digital, agar terciptanya kepastian hukum terhadap masyarakat yang menjalankan kegiatan ekonomi dan notaris dalam menjalankan jabatannya.</p>

This is an open access article under the [Lisensi Creative Commons Atribusi-BerbagiSerupa 4.0 Internasional](https://creativecommons.org/licenses/by-sa/4.0/)



Corresponding Author:

Muhammad Fernando,

Magister Kenotariatan Fakultas Hukum Universitas Indonesia

Email: muhamadfernandoo@gmail.com

1. PENDAHULUAN

A. Latar Belakang:

Perkembangan teknologi yang semakin pesat, membuat beberapa Norma Hukum juga harus meresponnya dengan cepat. Jika Norma Hukum terlambat dalam merespon perkembangan zaman, maka akan menimbulkan persoalan dan kebingungan dalam pelaksanaan norma hukum tersebut. Salah satu aspek yang mengalami perkembangan pesat akibat pengaruh teknologi adalah bidang perdagangan, yang sekarang dikenal sebagai *e-commerce*.

Aktivitas perdagangan melalui media internet saat ini lebih populer dengan *electronic commerce (e-commerce)* dan *e-bussines*. Perjanjian *e-commerce* misalnya, penerapan teknologi dalam perjanjian *e-contract* tidak seperti layaknya perjanjian pada umumnya, tetapi perjanjian tersebut dapat dilakukan meskipun tanpa adanya pertemuan langsung antara kedua belah pihak, namun perjanjian antar para pihak tersebut dilakukan secara elektronik.

Perjanjian dalam aktivitas *e-commerce* pada dasarnya sama dengan perjanjian yang dilakukan dalam transaksi perdagangan konvensional, akan tetapi perjanjian yang dipakai dalam *e-*

commerce merupakan perjanjian para pihak yang dibuat melalui sistem elektronik atau disebut kontrak elektronik.

Perjanjian antar pihak dapat dilakukan dengan hanya mengakses halaman web yang disediakan, berisi klausul atau perjanjian yang dibuat oleh pihak pertama (penjual), dan pihak yang lain (pembeli) hanya tinggal menekan tombol yang disediakan sebagai tanda persetujuan atas isi perjanjian yang telah ada, tanpa perlu membubuhkan tanda tangan seperti perjanjian pada umumnya, tetapi menggunakan tanda tangan elektronik atau digital signature. Sehingga para pihak tidak perlu bertemu langsung untuk mengadakan suatu perjanjian (e-date interchange). Mengingat tanda tangan digital berfungsi sebagai alat verifikasi dan autentifikasi. Selain itu Pasal 53 ayat (1) dan (2) Peraturan Pemerintah Nomor 82 Tahun 2010 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, menjelaskan bahwa, Tanda Tangan Elektronik berfungsi sebagai alat autentikasi dan verifikasi atas identitas penanda tangan, dan keutuhan dan keautentikan informasi elektronik. Sehingga, semakin banyak pelaku usaha maupun konsumen yang melakukan aktivitas ekonominya dengan melalui fasilitas elektronik, maka diperlukan norma hukum yang responsif untuk menjawab persoalan hukum dikemudian hari. Hal tersebut didasari karena transaksi konvensional, memiliki karakteristik yang berbeda dengan transaksi yang dilakukan secara online.

Oleh karena itu, idealnya Norma hukum yang ada, harus memberikan kepastian hukum guna memberikan payung hukum atas suatu perbuatan tertentu. Pikiran ini sejalan dengan yang disampaikan oleh Utrecht, bahwa teori kepastian hukum bertujuan untuk memberikan kesadaran bagi masyarakat untuk mengetahui mana yang boleh dilakukan dan mana yang dilarang.

Akan tetapi, keidealannya tidak terjadi jika tidak ada aturan yang mengatur mengenai Pihak yang berwenang menilai autentifikasi dari sebuah tanda tangan digital. Kekosongan hukum tersebut menimbulkan persoalan sebab, masing-masing Lembaga *Certification Authority*, dapat mengklaim hasil sertifikasi atas tanda tangan tertentu adalah valid, akan tetapi menurut Lembaga CA lain adalah tidak valid. Hal tersebut menimbulkan ketidakpastian yang serius bagi iklim hukum di Indonesia. Tidak adanya kepastian mengenai Lembaga/pihak mana yang berwenang menilai autentifikasi suatu tanda tangan digital, berpotensi tidak adanya keselarasan dalam membuktikan apakah tanda tangan digital tersebut asli atau tidak. Isu diatas yang hendak peneliti bahas dalam artikel ini.

2. METODE PENELITIAN

Penelitian ini menggunakan penelitian hukum yang bersifat normatif dengan jenis penelitian kepustakaan. Penelitian hukum normatif adalah penelitian hukum yang menggunakan data sekunder. Data Sekunder yang dicari lebih diutamakan kepada putusan-putusan mengenai Sertifikasi Notaris terhadap Transaksi yang dilakukan secara elektronik (*Cyber Notary*), data sekunder selain yang bersumber dari putusan juga dapat berasal dari kajian peraturan perundang-undangan dan penelitian kepustakaan yang berkaitan dengan topic penelitian. Data Sekunder berasal dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

3. HASIL PENELITIAN DAN PEMBAHASAN

Perkembangan Teknologi, membuat model transaksi berubah. Salah satu bentuk perubahan yang nampak adalah munculnya *e-commerce*. *E-commerce* merupakan perjanjian yang berbeda dengan perjanjian dalam model konvensional. Perjanjian elektronik adalah perjanjian yang para pihaknya bertransaksi melalui halaman web yang sudah disediakan. Halaman web tersebut berisikan mengenai klausul-klausul apa saja yang harus dipatuhi oleh pihak penjual dan pihak pembeli. Tanda dari adanya kesepakatan antara penjual dan pembeli adalah dengan ditekannya tombol yang telah disediakan, tanpa membubuhkan tanda tangan basah seperti perjanjian konvensional pada umumnya. Pada transaksi yang berbasis elektronik cukup menggunakan tanda tangan digital, sehingga para pihak yaitu penjual dan pembeli tidak perlu bertatap muka. Edmon Makarim menggunakan istilah kontrak elektronik (*elektronik contract*), bagi kontrak elektronik (*e-contract*) dan mendefinisikan kontrak online sebagai perikatan atau hubungan hukum yang dilakukan secara elektronik dengan memadukan jaringan (*networking*)

dari sistem informasi berbasis komputer dengan sistem komunikasi yang berdasar atas jaringan dan jasa telekomunikasi (*telecommunicated based*), yang selanjutnya difasilitasi oleh keberadaan jaringan internet.

E-signature atau tanda tangan digital, ataupun tanda tangan elektronik pada dasarnya adalah teknik dan mekanisme yang digunakan untuk memberikan kesamaan fungsi dan karakteristik tanda tangan tertulis (basah) yang dapat diterapkan dalam lingkungan elektronik (*functional equivalence approach*). Tanda tangan elektronik merupakan data dalam bentuk elektronik yang diletakkan, terasosiasi atau terkait dengan informasi elektronik yang berguna untuk mengidentifikasi penanda tangan dan menunjukkan persetujuan penanda tangan atas informasi elektronik yang dimaksud. Dengan kata lain, tanda tangan elektronik berfungsi sebagai alat verifikasi dan autentikasi.

Pada Pasal 53 ayat (1) dan (2) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, menjelaskan:

1. Tanda Tangan Elektronik berfungsi sebagai alat autentifikasi dan verifikasi atas:
 - a. Identitas Penanda Tangan
 - b. Keutuhan dan Keautentikan Informasi elektronik
2. Tanda Tangan Elektronik dalam Transaksi Elektronik merupakan persetujuan Penanda Tangan atas Informasi Elektronik dan/atau Dokumen Elektronik yang ditandatangani dengan Tanda Tangan Elektronik tersebut. Tanda tangan elektronik berdasarkan Pasal 53 ayat (2) Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, memiliki kekuatan hukum dan akibat hukum yang sah jika:
 - a. Data Pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan
 - b. Data Pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan hanya berada dalam kuasa Penanda Tangan
 - c. Segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui
 - d. Segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;
 - e. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penanda Tangannya dan
 - f. Terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait

Dalam prakteknya nanti apabila gagasan *cyber notary* maupun *E-notary* dapat diimplementasikan di Indonesia, maka kekuatan pembuktian informasi dan transaksi elektronik yang selama ini dipersepsikan sering kali mempunyai nilai pembuktian yang lemah maka akan menjadi lebih kuat kedudukannya karena dapat dipersepsikan sebagaimana layaknya akta autentik. Hal tersebut akan meningkatkan kepercayaan dan keamanan masyarakat terhadap transaksi elektronik.

Meskipun peluang notaris untuk berperan secara elektronik seakan tidak terlihat dalam UU notaris, namun sekiranya ada peraturan perundang-undangan lain yang memberikan peluang itu (contoh : PP yang diamanatkan UU ITE memberikan peluang bagi notaris untuk memberikan dukungan jasa layanan sertifikasi elektronik) Di dalam menjalankan tugasnya tersebut, telah dicantumkan dalam Pasal 15 ayat (3) Undang-undang Nomor 2 Tahun 2014 tentang perubahan atas Undang- undang Nomor 30 Tahun 2004 Tentang Peraturan Jabatan Notaris Lembaran Negara Republik Indonesia Tahun 2014 Nomor 3, Tambahan Lembaran Negara Nomor 5491 (yang selanjutnya disebut Undang undang Nomor 2 tahun 2014) yang berbunyi: “Selain kewenangan sebagaimana dimaksud pada ayat (1) dan ayat (2), Notaris mempunyai kewenangan lain yang diatur dalam peraturan perundangundangan.” Kewenangan lain yang dimaksud dalam Pasal tersebut, telah dijabarkan dalam penjelasan Pasal 15 ayat (3) Undang-undang Nomor 02 Tahun 2014 yang menyatakan bahwa: “Yang dimaksud dengan kewenangan lain yang diatur dalam peraturan perundang-undangan antara lain : kewenangan mensertifikasi transaksi yang dilakukan secara elektronik (*cyber notary*), membuat akta ikrar wakaf dan hipotik pesawat terbang”. Selain

itu, beberapa permasalahan hukum yang terkait dengan penyelenggaraan kerja notaris secara konvensional selama ini, juga akan terselesaikan dengan baik.

Teknologi-teknologi dan media-media baru semakin luas dipergunakan dalam praktek perdagangan, baik di tingkat nasional maupun internasional, sehingga organisasi-organisasi Internasional semakin memikirkan pengakuan hukum terhadap dokumen elektronik dan tanda tangan elektronik. Akhirnya, dorongan datang dari Komisi Perserikatan Bangsa-Bangsa untuk Hukum Dagang *Internasional United Nations Commission On International Trade Law, Model Law on Elektronik Commerce* (selanjutnya disebut UNCITRAL), mengeluarkan UNCITRAL *Model Law on Electronic Commerce* pada tanggal 16 Desember 1996. Model Law ini sesungguhnya diajukan untuk menawarkan model hukum kepada Negara-negara yang sudah ataupun belum mempunyai peraturan perundangundangan terhadap materi ini. Namun *Model law* sifatnya bebas, artinya Negara-negara dibiarkan bebas mau mengikutinya atau tidak. Berkat model law ini, banyak Negara di dunia berbenah diri, mereka memandang bahwa hukum pembuktian tradisional tidak mampu lagi beradaptasi dengan model perdagangan elektronik, pemerintahan elektronik serta pertukaran informasi yang cepat.

Oleh karena itu, sangat dibutuhkan produk hukum yang bertujuan untuk meningkatkan keamanan dari transaksi-transaksi elektronik melalui jaringan elektronik, serta untuk memberikan pengakuan terhadap kekuatan hukum dari alat bukti elektronik dan tanda tangan elektronik. Kenyataannya kegiatan cyber tidak lagi sederhana, karena kegiatannya tidak lagi dibatasi oleh teritorial suatu negara, yang mudah diakses kapanpun dan dari manapun. Kerugian dapat terjadi, baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat mudah untuk dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannya pun bisa demikian kompleks dan rumit. Sejak tahun 1999 Rancangan Undang-Undang ini dibahas oleh Badan Legislatif yang berwenang, akhirnya Indonesia mempunyai aturan hukum untuk mengatur masalah tersebut dengan dikeluarkannya Undang-Undang Nomor 11 tahun 2008, tentang “Informasi dan Transaksi Elektronik” yang disahkan pada tanggal 21 April 2008. Berdasarkan pada Pasal 18 juncto Pasal 7 juncto Pasal 11 Undang-Undang Nomor 11 Tahun 2008 maka kekuatan pembuktian dokumen elektronik tersebut yang ditandatangani dengan digital signature sama dengan kekuatan pembuktian akta otentik yang dibuat oleh pejabat umum yang berwenang. Aturan tersebut diatas bertentangan dengan Pasal 1 ayat (7) Undang-Undang Nomor 2 tahun 2014 yang dimaksud akta notaris adalah akta otentik yang dibuat oleh atau dihadapan Notaris menurut bentuk dan tata cara yang ditetapkan dalam Undang-Undang ini. Sedangkan pengertian akta otentik berdasarkan Pasal 1868 KUH Perdata adalah suatu akta yang didalam bentuk yang ditentukan oleh Undang- Undang, dibuat oleh atau di hadapan pegawai-pegawai umum yang berkuasa untuk itu di tempat di mana akta dibuatnya.

Akibat terjadi suatu pertentangan aturan tersebut, maka apabila salah satu pihak mengajukan gugatan dengan alat bukti dokumen elektronik yang ditandatangani dengan tanda tangan elektronik sebagai alat bukti, maka di dalam menyelesaikan sengketa dipengadilan, hakim dituntut untuk berani melakukan terobosan hukum, karena dia yang paling berkuasa dalam memutuskan suatu perkara dan karena dia juga yang dapat memberi suatu vonnis van de rechter, yang tidak langsung dapat didasarkan atas suatu peraturan hukum tertulis atau tidak tertulis. Dokumen elektronik yang ditandatangani dengan sebuah digital signature, dapat dikategorikan sebagai bukti tertulis. Tetapi, terdapat suatu prinsip hukum yang menyebabkan sulitnya pengembangan penggunaan dan dokumen elektronik atau digital signature, yakni adanya syarat bahwa dokumen tersebut harus dapat dilihat, dikirim dan disimpan dalam bentuk kertas.

Lembaga Verifikasi Tanda Tangan Digital Sebagai Penjamin Autentifikasi

Penerapan *cyber notary* notaris mengalami kendala salah satunya yaitu keharusan para penghadap untuk menandatangani akta, tanda tangan para pihak merupakan hal penting dalam suatu akta, karena tanda tangan pihak merupakan tanda bahwa para pihak setuju dengan seluruh

isi akta tersebut. Di Belanda sudah memulai untuk menggunakan tanda tangan elektronik dan mengaturnya dalam *richtlijnen elektronische handtekeningen* Tahun 1999, yang di dalamnya, untuk menjamin identifikasi originalitas tanda tangan tersebut dilakukan penitipan tanda tangan ke suatu lembaga independen disebut Trusted Third Party.

Trusted Third Party bertugas menyimpan tanda tangan digital, menjamin kebenaran pertukaran data dan menyimpan data lainnya dengan metode *orytografie*. Selain Belanda, Amerika Serikat juga mengeluarkan undang-undang *e-signature* yang mengatur tanda tangan elektronik dengan keabsahan yang sama dengan tanda tangan manual/biasa. Indonesia telah mempunyai peraturan mengenai tanda tangan elektronik yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik. Sekedar perbandingan, Di Belanda yang memiliki sistem hukum yang sama seperti Indonesia, notaris dapat menjadi pihak ketiga terpercaya dalam suatu transaksi elektronik (*trusted third party*) atau menjadi *escrow* untuk *source-code software computer*. Selain itu, notaris juga berperan penting dalam mencegah terjadinya penipuan (*fraud*). Sebutan *cybernotary* tidak hanya mengenai notaris modern yang menggunakan sistem komputerisasi dan jaringan internet untuk administrasi kantor, namun juga perluasan fungsi dan peran notaris dalam transaksi elektronik dan penyelenggaraan jabatannya secara elektronik.

C.A berkedudukan sebagai pihak ketiga yang dipercaya untuk memberikan kepastian atau pengesahan terhadap identitas dari seseorang atau pelanggan (klien C.A. tersebut). Selain itu C.A. juga mengesahkan pasangan kunci publik dan kunci privat milik orang tersebut. Proses sertifikasi untuk mendapatkan pengesahan dari C.A. dapat dibagi menjadi 3 tahap:

1. Pelanggan atau subscriber membuat sendiri pasangan kunci privat dan kunci publiknya dengan menggunakan *software* yang ada di dalam komputernya
2. Menunjukan bukti-bukti identitas dirinya sesuai dengan yang disyaratkan C.A
3. Membuktikan bahwa dia mempunyai kunci privat yang dapat dipasangkan dengan kunci publik tanpa harus memperlihatkan kunci privatnya.

Setelah persyaratan-persyaratan tersebut diuji keabsahannya maka C.A. menerbitkan sertifikat pengesahan (dapat berbentuk *hard-copy* maupun *soft-copy*). Sebelum diumumkan secara luas "*subscriber*" terlebih dahulu mempunyai hak untuk melihat apakah informasi-informasi yang ada pada sertifikat tersebut telah sesuai atau belum. Apabila informasi-informasi tersebut telah sesuai maka subscriber dapat mengumumkan sertifikat tersebut secara luas atau tindakan tersebut dapat diwakilkan kepada C.A. atau suatu badan lain yang berwenang untuk itu (suatu lembaga notariat). Selain untuk memenuhi sifat *integrity* dan *authenticity* dari sertifikat tersebut, C.A. akan membubuhkan *digital signature* miliknya pada sertifikat tersebut.

Sertifikat yang dikeluarkan oleh C.A tersebut berisi:

1. Identitas C.A. yang menerbitkannya.
2. Pemegang atau pemilik atau subscriber dari sertifikat tersebut.
3. Batas waktu keberlakuan sertifikat tersebut.
4. Kunci publik dari pemilik sertifikat.

Setelah sertifikat tersebut diumumkan maka pihak-pihak lain dapat melakukan transaksi, transfer pesan dan berbagai kegiatan dengan media internet secara aman dengan pihak pemilik sertifikat. Tanda tangan elektronik, memiliki cara kerja. Tanda tangan digital dibuat dengan menggunakan teknik kriptografi, suatu cabang dari matematika terapan yang menangani tentang pengubahan suatu informasi menjadi bentuk lain yang tidak dapat dimengerti dan dikembalikan seperti semula. Tanda tangan digital menggunakan "*public key cryptography*" (kriptografi kunci publik), dimana algoritmanya menggunakan dua buah kunci, yang pertama adalah kunci untuk membentuk tanda tangan digital atau mengubah data ke bentuk lain yang tidak dapat dimengerti, dan kunci kedua digunakan untuk verifikasi tanda tangan digital ataupun mengembalikan pesan ke bentuk semula.

Konsep ini juga dikenal sebagai "*assymmetric cryptosystem*" (sistem kriptografi non simetris). Sistem kriptografi ini menggunakan kunci privat, yang hanya diketahui oleh penandatanganan dan digunakan untuk membentuk tanda tangan digital, serta kunci publik, yang

digunakan untuk verifikasi tanda tangan digital. Jika beberapa orang ingin memverifikasi suatu tanda tangan digital yang dikeluarkan oleh seseorang, maka kunci publik tersebut harus disebarkan ke orang-orang tersebut. Kunci privat dan kunci publik ini sesungguhnya secara matematis ‘berhubungan’ (memenuhi persamaan-persamaan dan kaidah-kaidah tertentu).

Walaupun demikian, kunci privat tidak dapat ditemukan menggunakan informasi yang didapat dari kunci publik. Proses lain yang tak kalah penting adalah “fungsi hash”, digunakan untuk membentuk sekaligus memverifikasi tanda tangan digital. Fungsi *hash* adalah sebuah algoritma yang membentuk representasi digital atau semacam “sidik jari” dalam bentuk “nilai *hash*” (*hash value*) dan biasanya jauh lebih kecil dari dokumen aslinya dan unik hanya berlaku untuk dokumen tersebut. Perubahan sekecil apapun pada suatu dokumen akan mengakibatkan perubahan pada “nilai *hash*” yang berkorelasi dengan dokumen tersebut. Fungsi hash yang demikian disebut juga “fungsi *hash* satu arah”, karena suatu nilai hash tidak dapat digunakan untuk membentuk kembali dokumen aslinya. Oleh karenanya, fungsi hash dapat digunakan untuk membentuk tanda tangan digital. Fungsi hash ini akan menghasilkan “sidik jari” dari suatu dokumen (sehingga unik hanya berlaku untuk dokumen tersebut) yang ukurannya jauh lebih kecil daripada dokumen aslinya serta dapat mendeteksi apabila dokumen tersebut telah diubah dari bentuk aslinya. Penggunaan tanda tangan digital memerlukan dua proses, yaitu dari pihak penandatanganan serta dari pihak penerima. Secara rinci kedua proses tersebut dapat dijelaskan sebagai berikut:

1. Pembentukan tanda tangan digital menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat yang telah didefinisikan sebelumnya. Untuk dapat menjamin keamanan nilai hash maka seharusnya terdapat kemungkinan yang sangat kecil bahwa tanda tangan digital yang sama dapat dihasilkan dari dua dokumen serta kunci privat yang berbeda.
2. Verifikasi tanda tangan digital adalah proses pengecekan tanda tangan digital dengan mereferensikan ke dokumen asli dan kunci publik yang telah diberikan, dengan cara demikian dapat ditentukan apakah tanda tangan digital dibuat untuk dokumen yang sama menggunakan kunci privat yang berkorespondensi dengan kunci publik.

Untuk menandatangani sebuah dokumen atau informasi lain, penandatanganan pertamanya membatasi secara tepat bagian-bagian mana yang akan ditandatangani. Informasi yang dibatasi tersebut dinamakan “*message*”. Kemudian aplikasi tanda tangan digital akan membentuk nilai hash menjadi tanda tangan digital menggunakan kunci privat. Tanda tangan digital yang terbentuk adalah unikbaik untuk *message* dan juga kunci privat. Umumnya, sebuah tanda tangan digital disertakan pada dokumennya dan juga disimpan dengan dokumen tersebut juga. Bagaimanapun, tanda tangan digital juga dapat dikirim maupun disimpan sebagai dokumen terpisah, sepanjang masih dapat diasosiasikan dengan dokumennya. Karena tanda tangan digital bersifat unik pada dokumennya, maka pemisahan tanda tangan digital seperti itu merupakan hal yang tidak perlu dilakukan. Proses pembentukan dan verifikasi tanda tangan digital memenuhi unsur-unsur paling penting yang diharapkan dalam suatu tujuan legal, yaitu:

1. Otentikasi Penandatanganan: Jika pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah yang telah didefinisikan, maka tanda tangan digital akan dapat menghubungkan atau mengasosiasikan dokumen dengan penandatanganan. Tanda tangan digital tidak dapat dipalsukan, kecuali penandatanganan kehilangan kontrol dari kunci privat miliknya.
2. Otentikasi Dokumen: Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan tingkat kepastian dan ketepatan yang jauh lebih tinggi daripada tanda tangan di atas kertas.
3. Penegasan: Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatanganan. Tindakan ini dapat menegaskan bahwa penandatanganan setuju dan bertanggung jawab terhadap isi dokumen.
4. Efisiensi: Proses pembentukan dan verifikasi tanda tangan
5. digital menyediakan tingkat kepastian yang tinggi bahwa tanda tangan yang ada merupakan tanda tangan sah dan asli dari pemilik kunci privat.

Dengan tanda tangan digital , tidak perlu ada verifikasi dengan melihat secara teliti (membandingkan) antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya seperti yang biasa dilakukan dalam pengecekan tanda tangan secara manual. Menurut hemat penulis, dengan diaturnya mengenai Lembaga mana yang berwenang untuk menilai autentifikasi tanda tangan digital, maka akan memunculkan kepastian hukum bagi pelaku usaha serta notaris sebagai profesi yang berhubungan langsung dengan beberapa kegiatan usaha secara digital.

4. KESIMPULAN

Berdasarkan analisis diatas, ditemukan bahwa adanya kekosongan Norma terkait penentuan Lembaga/Pihak yang berwenang dalam menilai autentifikasi Tanda Tangan Digital dalam transaksi *E-Commerce*. Tidak diaturnya mengenai Lembaga yang berwenang dalam menilai autentifikasi tersebut menyebabkan tidak adanya standart baku dalam menilai apakah tanda tangan digital yang tertera dalam suatu perjanjian adalah asli atau tidak. Sehingga perlu dibuat mengenai norma yang mengatur adanya Lembaga yang bertugas untuk menilai keaslian dan Riwayat tanda tangan digital, agar terjaminnya kepastian hukum bagi konsumen, serta Notaris sebagai profesi yang banyak terlibat dalam pembuatan akta yang mengahsruskan adanya tanda tangan elektronik. Sehingga berpijak dari persoalan diatas, maka diperlukannya norma yang mengatur mengenai Lembaga independen sebagai standart baku dalam menilai autentifikasi dari tanda tangan digital.

5. DAFTAR PUSTAKA

- Cita Yustia Sefriani, et. al. Buku Pintar Bisnis Online dan Transaksi Elektronik, (Jakarta: Gramedia Pustaka, 2013). Hlm. 101
- Emma Nurita, Cyber Notary Pemahaman Awal dalam Konsep Pemikiran, Refika Aditama, Bandung, 2012, hlm. 53.
- Henry Arianto, Hukum Responsif dan Penegakan Hukum di Indonesia, Lex Jurnalica Volume 7 Nomor2, April 2010
- Herlien Budiono, Kumpulan Tulisan Hukum Perdata di Bidang Kenotariatan, Bandung: Citra Aditya Bakti, 2008. hlm 221
- Josua Sitompul, Cyberspace, Cybercrime, Cyberlaw, Jakarta: Tatanusa, 2012. Hlm 92
- Mario Julyano and Aditya Yuli Sulistyawan, "Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum," *Crepido* 1, no. 1 (2019): 13–22, <https://doi.org/https://doi.org/10.14710/>.
- Rudyanti Dorotea Tobing. Aspek-Aspek Hukum Bisnis, Pengertian, Asas, Teori dan Praktik. (Yogyakarta: Lasbang Justia, 2012) Hlm. 216