BAB II

TINJAUAN UMUM

A. Tinjauan Umum Tentang Tanda Tangan Elektronik

1. Pengertian tanda tangan elektronik,

Pengertian tanda tangan elektronik berdasarkan pada Pasal 1 ayat (12) Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik adalah sebagai berikut : "Tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi". Penanda tangan adalah subjek hukum yang terasosiasi atau terkait dengan tanda tangan elektronik. Definisi tersebut mencakup suatu anggapan, bahwa pada pernyataan yang dibuat secara tertulis harus dibubuhkan tanda tangan dari yang bersangkutan. Digital signature, adalah sebuah pengaman pada data digital yang dibuat dengan kunci tanda tangan pribadi (private signature key), yang penggunaannya tergantung pada kunci publik (public key) yang menjadi pasangannya. Menurut Julius Indra Dwiparyo, tanda tangan elektronik, adalah sebuah identitas elektronik yang berfungsi sebagai tanda persetujuan terhadap kewajiban-kewajiban yang melekat pada sebuah akta elektronik.[37]

Informasi elektronik yang menggunakan jaringan publik, bisa saja seseorang berniat jahat mengganti informasi elektronik yang telah ditandatangani oleh para pihak dengan informasi elektronik lain tetapi tanda tangan tidak berubah. Pada data elektronik perubahan ini mudah terjadi dan

[37] Julius Indra Dwipayono, *Tanda Tangan Elektronik Dalam Hukum Indonesia*, 2005, www.legalitas.org

tidak mudah dikenali. Oleh karena itu, tanda tangan elektronik harus terasosiasi dengan informasi elektronik. Terasosiasi adalah informasi elektronik yang ingin ditandatangani menjadi data pembuatan tanda tangan elektronik, dengan demikian, antara tanda tangan elektronik dan informasi elektronik yang ditandatangani menjadi erat hubungannya seperti fungsi kertas. Keuntungannya adalah jika terjadi perubahan informasi elektronik yang sudah ditandatangani maka tentu tanda tangan elektronik juga berubah.[38]

Tanda tangan elektronik bukan tanda tangan yang dibubuhkan di atas kertas sebagaimana lazimnya suatu tanda tangan, tanda tangan elektronik diperoleh dengan terlebih dahulu meciptakan suatu message *digest* atau *hast*, yaitu *mathematical summary* dokumen yang dikirimkan melalui cyberspace.[39]

Tanda tangan elektronik pada prinsipnya berkenaan dengan jaminan untuk message integrity yang menjamin bahwa si pengirim pesan (sender) adalah benar-benar orang yang berhak dan bertanggung jawab untuk itu. Hal ini berbeda dari tanda tangan biasa yang berfungsi sebagai pengakuan dan penerimaan atas isi pesan atau dokumen. Tanda tangan elektronik adalah sebuah item data yang berhubungan dengan sebuah pengkodean pesan digital yang dimaksudkan untuk memberikan kepastian tentang keaslian data dan memastikan bahwa data tidak termodifikasi.[40] Persoalan hukum yang muncul sekitar hal ini antara lain berkenaan dengan fungsi dan kekuatan hukum tanda

[38] Ronny, *Sembilan Peraturan Pemerintah Dan Dua Lembaga Yang Baru UndangUndang Informasi Transaksi Elektronik*, www.ronny-hukum.blogspot.com, 2008, Hlm.3

[39] Soemarno Partodihardjo, *Tanya Jawab Sekitar Undang-Undang No.11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*, PT Gramedia Pustaka Utama, Jakarta, 2009, Hlm. 20.

[40] *Ibid.*, Hlm. 21.

tangan elektronik. Di Amerika Serikat saat ini telah ditetapkan satu undang-undang yang secara formal mengakui keabsahan tanda tangan elektronik. Pengaturan di tingkat internasional diatur dalam Pasal 7 UNICITRAL Model Law (The United Nations Commissions on International Trade Law) merupakan salah satu organisasi internasional yang pertama kali mulai membahas mengenai perkembangan telematika informatika dan dampaknya terhadap perkembangan elektronik.

Tujuan Tanda Tangan Digital, tujuan dari suatu tanda tangan dalam suatu dokumen elektronik adalah sebagai berikut :

a. Untuk memastikan otensitas dari dokumen tersebut;
b. Untuk menerima atau menyetujui secara menyakinkan isi dari sebuah tulisan.

Sifat persyaratan digital signature atau tanda tangan elektronik, yaitu :[41]

a. Autentik
b. Aman
c. Interoperabilitas dari perangkat lunak maupun jaringan dari penyedia jasa.
d. Konfidensialitas.
e. Hanya sah untuk dokumen itu saja atau kopinya yang sama persis.
f. Dapat diperiksa dengan mudah.
g. Divisibilitas, berkaitan dengan spesifikasi praktis transaksi baik untuk volume besar atau skala kecil.

[41] *Loc.cit*, Hlm. 91-92.

Sedangkan Manfaat Tanda Tangan Digital (Digital Signature) adalah suatu tanda tangan digital (digital Signature) akan menyebabkan data elektronik yang dikirimkan melalui open network tersebut menjadi terjamin, sehingga mempunyai manfaat dari digital signature adalah sebagai berikut:[42]

a. *Authenticity*

Dengan memberikan *digital signature* pada data elektronik yang dikirimkan, maka akan dapat atau bisa ditunjukkan darimana data-data elektronik tersebut sesungguhnya berasal. Terjaminnya integritas pesan tersebut bisa terjadi, karena keberadaan dari *digital certificate*. *Digital Certificate* diperoleh, atas dasar aplikasi kepada *Certification Authority* oleh *user* atau *subscriber*. Digital Certificate berisi informasi mengenai pengguna antara lain:

- Identitas
- Kewenangan
- Kedudukan hukum
- Status dari user atau pengguna

Digital certificate ini memiliki berbagai tingkatan atau level, tingkatan dari digital certificate ini menentukan berapa besar kewenangan yang dimiliki oleh pengguna. Contoh dari kewenangan atau kwalifikasi ini adalah apabila suatu perusahan hendak melakukan perbuatan hukum, maka pihak yang berwenang mewakili perusahaan tersebut adalah direksi. Jadi apabila suatu perusahaan hendak melakukan suatu perbuatan hukum maka *digital certificate* yang

[42] Arrianto Mukti Wibowo, dkk, *Op.Cit*.**,** Hlm. 5

dipergunakan adalah *digital certificate* yang dipunyai oleh direksi perusahaan tersebut.

Dengan keberadaan dari digital certificate ini maka pihak ketiga yang berhubungan dengan pemegang digital certificate tersebut dapat merasa yakin bahwa suatu pesan adalah benar berasal dari pengguna tersebut.

b. *Integrity*

Penggunaan digital signature yang diaplikasikan pada pesan atau data elektronik yang dikirimkan, dapat menjamin bahwa pesan atau data elektronik tersebut tidak mengalami suatu perubahan atau modifikasi oleh pihak yang tidak berwenang.

Integritas atau *integrity* berhubungan dengan masalah keutuhan dari suatu data yang dikirimkan. Seorang penerima pesan atau data dapat merasa yakin apakah pesan yang diterimanya sama dengan pesan yang dikirimkan. Ia dapat merasa yakin bahwa data tersebut pernah dimodifikasi atau diubah selama proses pengiriman atau penyimpanan. Jaminan *authenticity* ini dapat dilihat dari adanya *hash function* dalam sistem *digital signature*, dimana penerima data *(recipient)* dapat melakukan pembandingan *hash value*. Apabila *hash value*-nya sama dan sesuai, maka data tersebut benar-benar otentik, tidak pernah terjadi suatu tindakan yang sifatnya merubah (*modify*) dari data tersebut pada saat proses pengiriman, sehingga terjamin *authenticity*-nya. Sebaliknya apabila *hash value*-nya berbeda, maka patut dicurigai dan langsung dapat disimpulkan bahwa recipient menerima data yang telah dimodifikasi.

c. *Non-Repudiation* (Tidak Dapat Disangkal Keberadaannya)

Non-Repudiation (Tidak Dapat Disangkal Keberadaannya), timbul dari keberadaan digital signature yang menggunakan enkripsi asimetris (*asymmetric encryption*). *Enskripsi asimetris* ini melibatkan keberadaan dari kunci privat dan kunci publik. Suatu pesan yang telah dienkripsi dengan menggunakan kunci privat, maka ia hanya dapat dibuka/dekripsi dengan menggunakan kunci publik dari pengirim. Jadi apabila terdapat suatu pesan yang telah dienkripsi oleh pengirim dengan menggunakan kunci privatnya, maka ia tidak dapat menyangkal keberadaan pesan tersebut, karena terbukti bahwa pesan tersebut didekripsi dengan kunci publik pengirim. Keutuhan dari pesan tersebut dapat dilihat dari keberadaan *hash function* dari pesan tersebut, dengan catatan bahwa data yang telah di-sign akan dimasukkan ke dalam *digital envelope*.

Non-repudiation (Tidak dapat disangkalnya keberadaan) suatu pesan berhubungan dengan orang yang mengirimkan pesan tersebut Pengirim pesan tidak dapat menyangkal bahwa ia telah mengirimkan suatu pesan apabila ia sudah mengirimkan suatu pesan. Ia juga tidak dapat menyangkal isi dari suatu pesan berbeda dengan apa yang ia kirimkan apabila ia telah mengirim pesan tersebut. Non repudiation adalah hal yang sangat penting bagi e-commerce apabila suatu transaksi dilakukan melalui suatu jaringan internet, kontrak elektronik (electronic contracts), ataupun transaksi pembayaran.

d. *Confidentiality*

Pesan dalam bentuk data elektronik yang dikirimkan tersebut bersifat rahasia atau confidental, sehingga tidak semua orang dapat mengetahui isi data elektronik yang telah di*sign* dan dimasukkan dalam digital envolve. Keberadaan

digital envolve yang termasuk bagian yang integral dari digital signature, menyebabkan suatu pesan yang telah dienkripsi hanya dapat dibuka oleh orang yang berhak. Tingkat kerahasiaan dari suatu pesan yang telah dienkripsi ini, tergantung dari panjang kunci atau key yang dipakai untuk melakukan enkripsi.

Pengamanan data dalam e-commerce dengan metode kriptografi melalui skema digital signature tersebut secara teknis sudah dapat diterima dan diterapkan, namun apabila kita bahas dari sudut pandang ilmu hukum ternyata masih kurang mendapatkan perhatian. Kurangnya perhatian dari ilmu hukum dapat dimengerti karena, khususnya di Indonesia, penggunaan komputer sebagai alat komunikasi melalui jaringan internet baru dikenal semenjak tahun 1994. Dengan demikian pengamanan jaringan internet dengan metode digital signature di Indonesia tentu masih merupakan hal yang baru bagi kalangan pengguna komputer.

2. Keabsahan Tanda Tangan elektronik

Konsep "tanda tangan digital" (digital signature) yang dikenal pada dunia keamanan komputer adalah hasil dari penerapan teknik-teknik komputer pada suatu informasi. Sedangkan di dunia umum, tanda tangan mempunyai arti yang lebih luas, yaitu sebarang tanda yang dibuat dengan maksud untuk melegalisasi dokumen yang ditandatangani. Dalam dunia nyata, untuk menjamin keaslian serta legalitas suatu dokumen digunakan tanda tangan. Tanda tangan ini merupakan suatu tanda yang bersifat unik milik seseorang dan digunakan untuk memberi pengesahan bahwa orang tersebut setuju dan mengakui isi dari dokumen yang ditandatangani. Untuk dokumen-dokumen elektronik pun dibutuhkan hal semacam ini. Oleh karena itu, diciptakan suatu sistem otentikasi yang disebut

tanda tangan digital. Tanda tangan digital merupakan suatu cara untuk menjamin keaslian suatu dokumen elektronik dan menjaga supaya pengirim dokumen dalam suatu waktu tidak dapat menyangkal bahwa dirinya telah mengirimkan dokumen tersebut. Tanda tangan digital menggunakan algoritma-algoritma serta teknik-teknik komputer khusus dalam penerapannya.

Berbicara mengenai keabsahan tanda tangan elektronik, suatu tanda tangan elektronik pasti diperoleh dengan adanya suatu transaksi, orang selalu akan mendasarkan pada ketentuan dalam Pasal 1320 Kitab Undang-undang Hukum Perdata yang menyatakan bahwa untuk sahnya suatu perjanjian diperlukan 4 (empat) syarat, yakni:

a) Sepakat mereka yang mengikatkan dirinya;
b) Cakap untuk membuat suatu perikatan;
c) Hal tertentu;
d) Sebab yang halal.

Dengan mendasarkan pada ketentuan Pasal 1320 KUHPerdata sebenarnya tidak dipermasalahkan mengenai media yang digunakan dalam transaksi, atau dengan kata lain Pasal 1320 KUHPerdata tidak mensyaratkan bentuk dan jenis media yang digunakan dalam bertransaksi. Oleh karena itu, dapat saja dilakukan secara langsung maupun secara elektronik. Namun suatu perjanjian dapat dikatakan sah bila telah memenuhi unsur-unsur sebagaimana dimaksud dalam Pasal 1320 tersebut. Demikian pula asas kebebasan berkontrak yang dianut KUHPerdata, dimana para pihak dapat bebas menentukan dan membuat suatu perikatan atau perjanjian dalam bertransaksi yang dilakukan dengan itikad baik

(PasaL 1338). Jadi apapun bentuk dan media dari kesepakatan tersebut, tetap berlaku dan mengikat para pihak karena perikatan tersebut merupakan undang-undang bagi yang membuatnya. Permasalahan akan timbul dari suatu transaksi bila salah satu pihak ingkar janji. Penyelesaian permasalahan yang terjadi tersebut, selalu berkaitan dengan apa yang menjadi bukti dalam transaksi, lebih-lebih bila transaksi menggunakan sarana elektronik.[43] Hal ini karena penggunaan dokumen atau data elektronik sebagai akibat transaksi melalui media elektronik, belum secara khusus diatur dalam hukum acara yang berlaku, baik dalam Hukum Acara Perdata maupun dalam Hukum Acara Pidana. Mengenai hukum materiilnya pada dasarnya sudah secara tegas diatur dalam Pasal 15 ayat (1) Undang- Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan yang menyatakan bahwa "dokumen perusahaan yang telah dimuat dalam microfilm atau media lainnya dan atau hasil cetaknya merupakan alat bukti yang sah". Selanjutnya apabila kita perhatikan ketentuan dalam Pasal 1 angka 2 mengenai pengertian dokumen dan dikaitkan dengan ketentuan Pasal 12 ayat (1) dan ayat (2) Undang-Undang Nomor 8 Tahun 1997 jo. Pasal 1320 KUHPerdata, transaksi melalui media elektronik adalah sah menurut hukum.

KUH Perdata menjelaskan maksud hal tertentu, dengan memberikan rumusan dalam Pasal 1333 KUH Perdata, yang berbunyi sebagai berikut: "Suatu perjanjian harus mempunyai sebagai pokok perjanjian berupa suatu kebendaan yang paling sedikit ditentukan jenisnya. Tidaklah menjadi halangan bahwa jumlah kebendaan tidak tentu, asal saja jumlah itu kemudian dapat ditentukan atau

[43]Barkatullah, Abdul Prasetyo., Halim Teguh, *Bisnis E-commerce Studi Sistem Keamanan Dan Hukum Di Indonesia*, Pustaka Pelajar, Jakarta, 2005

dihitung". Secara sepintas, dengan rumusan "pokok perjanjian berupa barang yang telah ditentukan jenisnya, tampaknya KUH Perdata hanya menekankan pada perikatan untuk memberikan atau menyerahkan sesuatu. Namun demikian jika kita perhatikan lebih lanjut, rumusan tersebut hendak menegaskan kepada kita semua bahwa apapun jenis perikatannya, baik itu perikatan untuk memberikan sesuatu, berbuat sesuatu, atau untuk tidak berbuat sesuatu, KUH Perdata hendak menjelaskan, bahwa semua jenis perikatan tersebut pasti melibatkan keberadaan atau eksistensi dari suatu kebendaan yang tertentu. Perjanjian yang diperjanjikan harus suatu hal atau suatu barang yang cukup jelas atau tertentu. Syarat ini perlu untuk dapat menetapkan kewajiban dari si berhutang jika ada perselisihan. Barang yang dimaksudkan dalam perjanjian paling sedikit harus ditentukan jenisnya. Bahwa barang itu sudah ada atau sudah berada di tangannya si berhutang pada waktu perjanjian dibuat, tidak diharuskan oleh undang-undang. Juga jumlahnya tidak perlu disebutkan, asal saja kemudian dapat dihitung atau ditetapkan. Syarat bahwa prestasi harus tertentu atau dapat ditentukan, gunanya ialah untuk menetapkan hak dan kewajiban kedua belah pihak, jika timbul perselisihan dalam pelaksanaan perjanjian. Jika prestasi kabur atau dirasakan kurang jelas, yang menyebabkan perjanjian itu tidak dapat dilaksanakan, maka dianggap tidak ada obyek perjanjian dan akibat hukum perjanjian itu batal demi hukum.[44]

Undang-undang Informasi dan Transaksi Elektronik (UU ITE) memiliki asas diantaranya netral teknologi atau kebebasan memilih teknologi. Hal ini termasuk memilih jenis tanda tangan elektronik yang dipergunakan untuk

[44] Rosa Agustina T. Pangaribuan, *Op.Cit*., Hlm.1

menandatangani suatu informasi elektronik dan/atau dokumen elektronik. Asas netral teknologi dalam UU ITE perlu dipahami secara berhati-hati, dan para pihak yang melakukan transaksi elektronik sepatutnya menggunakan tanda tangan elektronik yang memiliki kekuatan hukum dan akibat hukum yang sah seperti diatur dalam pasal 11 ayat 1 UU ITE.

Keabsahan Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut berdasarkan Pasal 11 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, yaitu :

a) Data pembuatan tanda tangan elektronik terkait hanya kepada penanda tangan.
b) Data pembuatan tanda tangan elektronik pada saat proses
c) penanda tangan elektronik hanya berada dalam kuasa penanda tangan.
d) Segala perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui.
e) Segala perubahan terhadap informasi elektronik yang terkait dengan tanda tangan elektronik tersebut setelah waktu penanda tanganan dapat diketahui.
f) Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penanda-tangannya.
g) Terdapat cara tertentu untuk menunjukkan bahwa penanda tangan telah memberikan persetujuan terhadap informasi

elektronik yang terkait.

3. Klasifikasi Tanda Tangan Elektronik

a. Tanda Tangan Elektronik (Biasa)

Tanda tangan elektronik biasa, sesuai dengan pengertian mengenai tanda tangan elektronik diatas adalah tanda tangan yang ditujukan merujuk kepada si penanda tangan, yang dilakukan dengan media elektronik. Contoh paling mudah adalah suatu tanda tangan konvensional (tertulis) yang kemudian di-scan. Kemudian hasil scan tersebut akan menjadi suatu informasi elektronik, biasanya berupa suatu file gambar, ditempelkan (paste) pada suatu dokumen elektronik. Hal tersebut sudah termasuk dalam ruang lingkup tanda tangan elektronik (biasa).

b. Tanda Tangan Elektronik yang Aman (*Secure atau Reliable*)

Tanda tangan elektronik yang aman atau Electronic Signature, merupakan suatu tanda tangan elektronik yang harus memenuhi persyaratan-persyaratan tertentu, sehingga dapat dalam konteks kesamaanya, dapat dipersamakan dengan tanda tangan konvensional. Tanda tangan elektronik yang aman ini diperuntukkan untuk menampung semua jenis kemajuan teknologi yang mungkin berkembang dalam bidang keamanan terhadap informasi elektronik yang aman ditujukan untuk tidakhanya dapat merujuk kepada si penanda tangan, tetapi juga untuk menjaga keutuhan dan keamanan daripada suatu informasi elektronik yang dilekatkan. Tanda tangan digital termasuk di dalam kategori tanda tangan elektronik yang aman.

B. Tinjauan Umum Tentang Kontrak Elektronik (*E-Contract*)

1. Pengertian Kontrak elektronik

Pada hakekatnya kontrak elektronik adalah perjanjian yang disepakati para pihak yang membuatnya hanya medium atau sarananya sangat berbeda, menggunakan sistem elektronik. Keabsahan suatu kontrak elektronik ini ternyata ditegaskan Undang-undang ITE pada pasal 5 ayat (3) dengan mensyaratkan keabsahan kontrak (dokumen elektronik) bila menggunakan sistem elektronik yang sudah disertifikasi sebagaimana diatur dalam pasal 13 sampai dengan 16 Undang-undang ITE.

2. Dokumen elektronik

Dokumen elektronik berdasarkan pada pasal 1 ayat 4 UndangUndang Nomor 19 Tahun 2016 adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, atau sejenisnya, huruf, tanda, angka, kode akses, symbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu memahaminya. Dokumen elektronik dapat dijadikan alat bukti yang sah, menurut Undang-undang Informasi dan Transaksi Elektronik, suatu dokumen elektronik dinyatakan sah untuk dijadikan alat bukti apabila menggunakan sistem elektronik yang andal dan aman, serta memenuhi persyaratan minimum sebagai berikut :

a. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan;

b. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan system elektronik tersebut;
c. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut;
d. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik tersebut; dan
e. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Dokumen elektronik merupakan dokumen yang terjadi akibat suatu transaksi komersial elektronik (e-commerce). Untuk menentukan kapan terjadinya kesepakatan dalam suatu transaksi komersial elektonik (ecommrce). Hasil print out dari sebuah dokumen elektronik yang dihasilkan dalam pertukaran informasi, selayaknya memiliki nilai pembuktian yang sama seperti bukti tulisan lainnya. Dalam memutus suatu perkara, tentu saja hakim harus mendasarkan ketentuan hukum acara yang mengatur masalah pembuktian.

3. Transaksi Komersial Elektronik (*E-Commerce*)

a. Pengertian Transaksi Komersial Elektronik

Transaksi komersial elektronik, merupakan salah satu bentuk bisnis modern yang bersifat non-face dan non-sign (tanpa bertatap muka dan tanpa tanda tangan). Transaksi komersial elektronik (*e-commerce*) memiliki beberapa ciri

khusus, diantaranya bahwa transaksi ini bersifat *paperless* (tanpa dokumen tertulis), *borderless* (tanpa batas geografis) dan para pihak yang melakukan transaksi tidak perlu bertatap muka. Transaksi komersial elektronik (e-commerce), mengacu kepada semua bentuk transaksi komersial yang didasarkan pada proses elektronis dan transmisi data melalui media elektronik. Karena itu, tidak ada definisi konsep transaksi komersial elektronik yang berlaku Internasional.

Hal serupa juga dikemukakan oleh UNCITRAL yang mendefinisikan *e-commerce* sebagai berikut : "Electronic commerce. Which involves the use of alternatives to paper-based of communication and storage of information".[45]

Vladimir Zwass, mendefinisikan transaksi komersial elektronik (*e-commerce*) sebagai pertukaran informasi bisnis, mempertahankan hubungan bisnis dan melalukan transaksi bisnis melalui jaringan komunikasi.[46] Mengamati hal tersebut, transaksi komersial elektronik (*e-commerce*) adalah transaksi perdagangan jual beli barang dan jasa yang dilakukan dengan cara pertukaran informasi atau data menggunakan alternatif selain media tertulis, yang dimaksud media transaksi di sini adalah media elektronik, khususnya internet.

Transaksi Elektronik berdasarkan pada Pasal 1 ayat (9) UndangUndang Nomor 19 tahun 2016 tentang Informasi Transaksi Elektronik menyebutkan : Transaksi elektronik, adalah hubungan hukum yang dilakukan melalui komputer, atau media elektronik lainnya. Berdasarkan berbagai definisi tersebut, terdapat beberapa kesamaan yaitu :

---

[45] Ridwan Khairandy, *Pembaharuan Hukum Kontrak Sebagai Antisipasi Transaksi Elektronic Commerce "become a popular prefixs for other terms associated with electronic Transaction"* , Jurnal Hukum Bisnis, vol.16, 2001, Hlm. 57.

[46] *Ibid*, Hlm. 65

1) Terdapat transaksi antara dua pihak atau lebih;
2) Ada pertukaran barang dan jasa;
3) Menggunakan internet sebagai medium utama untuk melakukan transaksi.

Transaksi komersial elektronik (e-commerce), pada prinsipnya merupakan hubungan hukum berupa pertukaran barang dan jasa antara penjual dan pembeli yang memiliki prinsip dasar sama dengan transaksi konvensional, namun dilaksanakan dengan pertukaran data melalui media yang tidak berwujud (internet), di mana para pihak tidak perlu bertatap muka secara fisik.

b. Jenis Transaksi Komersial Elektronik (*E-commerce*)

Secara garis besar jenis transaksi komersial elektronik (*e-commerce*) dibagi menjadi 5, yaitu:[47]

a. *Business to Business* (B2B)

Transaksi B2B merupakan transaksi, di mana kedua belah pihak yang melakukan transaksi adalah suatu perusahaan.

b. *Busines to Consumer* (B2C)

Transaksi B2C, merupakan transaksi antara perusahaan dengan konsumen atau individu. Transaksi B2C meliputi pembelian produk secara langsung oleh konsumen melalui internet.

c. *Customer to Customer* (C2C)

Transaksi C2C merupakan transaksi, di mana individu saling menjual barang satu sama lain.

[47] Roberto Aaron, *Electronic commerce :Enablers and Implications*, IEEE Communication Magazine, 1999, Hlm. 47.

d. *Costumer to Business* (C2B)

Transaksi C2B, merupakan transaksi yang memungkinkan individu menjual barang pada perusahaan.

e. *Customer to Government* (C2G)

Transaksi C2G merupakan transaksi, di mana individu dapat melakukan transaksi dengan pemerintah.

4. Sertifikat Elektronik

Sertifikat elektronik menduduki peran layaknya "paspor elektronik", ia tidak dapat dipisahkan dari praktek tanda tanga elektronik, ia membawa kekuatan hukum yang kuat karena dapat meyakinkan identitas Penandatangan.[48] Sertifikat elektronik mempunyai sebuah struktur internal, artinya ada beberapa bagian yang diwajibkan untuk diinformasikan atau dilekatkan pada sertifikat tersebut untuk memberikan kekuatan hukum pada sertifikat tersebut.

Penyelenggaraan Sertifikasi Elektronik menurut Pasal 13 dan 14 UU.ITE, yaitu :

a. Setiap orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan tanda tangan elektronik.
b. Penyelenggara Sertifikasi Elektronik harus memastikan suatu tanda tangan elektronik dengan pemiliknya.
c. Penyelenggara Sertifikasi Elektronik terdiri atas Penyelenggara Sertifikasi Elektronik Indonesia dan Penyelenggara Sertifikat Elektronik Asing.

[48] Julien ESNAULT, *Memoire : la signature électronique, D.E.S.S. du droit du Multimédia et de l'Informatique, Université de Paris II Pantheon-Assas*, Paris, Année universitaire 2002-2003, hlm.11. www.legalitas.org

d. Penyelenggara Sertifikasi Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.
e. Penyelenggara Sertifikasi Elektronik Asing yang beroperasi di Indonesia harus terdaftar di Indonesia.
f. Ketentuan lenih lanjut mengenai Penyelenggara Sertifikasi Elektronik diatur dengan Peraturan Pemerintah (PP).

Penyelenggara Sertifikasi Elektronik harus menyediakan informasi yang akurat jelas, dan pasti kepada setiap pengguna jasa, yang meliputi :

a. Metode yang digunakan untuk mengidentifikasikan Penanda Tangan.
b. Hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda Tangan Elektronik.
c. Hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik.

Penjelasannya adalah informasi yang minimum harus dipenuhi oleh setiap penyelenggara Tanda Tangan Elektronik.

5. *Certification Authority* (CA)

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 menjad 3 tahap :

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

Tahapan-tahapan tersebut tidak mutlak harus seperti di atas, akan tetapi tergantung pada ketentuan-ketentuan yang telah ditetapkan oleh C.A. itu sendiri. Hal ini berkaitan dengan level atau tingkatan dari sertifikat yang diterbitkannya dan level atau tingkatan ini berkaitan juga dengan besarnya kewenangan yang diperoleh pelanggan "Subscriber" berdasarkan sertifikat yang didapatkannya. Semakin besar kewenangannya yang diperoleh dari suatu Digital Certificate yang diterbitkan oleh C.A. semakin tinggi pula level sertifikat yang diperoleh serta semakin ketat pula persyaratan yang ditetapkan oleh C.A. Sebagai contoh; untuk mendapatkan suatu sertifikat yang mempunyai level kewenangan yang cukup tinggi, terkadang C.A. bahkan memerlukan kehadiran secara fisik si "subscriber" sehingga C.A. dapat memperoleh kepastian pihak yang akan memperoleh sertifikat tersebut.

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 informasiinformasi 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.[49]

Informasi-informasi yang terdapat di dalam sertifikat tersebut diantaranya dapat berupa :

a. Identitas C.A. yang menerbitkannya.
b. Pemegang atau pemilik atau subscriber dari sertifikat tersebut.
c. Batas waktu keberlakuan sertifikat tersebut.
d. 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. Fungsi C.A.

Fungsi-fungsi C.A yang telah disebutkan di atas dapat digolongkan sebagai berikut :

a. Membentuk hierarki bagi penandatanganan digital.
b. Mengumumkan peraturan-peraturan mengenai penerbitan sertifikat.
c. Menerima dan memeriksa pendaftaran yang diajukan.

[49] *http://en.wikipedia.org/wiki/Public_key_infrastructure*, diakses September 2018

Selain itu, pihak-pihak yang terlibat dalam e-commerce tidak hanya dilihat pada statusnya sebagai pihak, melainkan juga dengan melihat kedudukannya dalam perikatan, yaitu sebagai berikut:

a. Penjual (merchant)
b. Pembeli (buyer)
c. Certification Authority (CA)
d. Account Issuer (penerbit rekening contoh: kartu kredit)
e. Jaringan pembayaran (contohnya Visa dan Mastercard dalam scheme SET)
f. Internet Service Provider (ISP)
g. Internet Backbones
h. Aspek Kontrak Perdagangan Internasional.