UNIVERSITAS INDONESIA

TANGGUNG JAWAB HUKUM PENYELENGGARA TANDA TANGAN DIGITAL TERSERTIFIKASI YANG BERINDUK (ANALISA KOMPARATIF TERHADAP KASUS DIGINOTAR DI BELANDA)

TESIS

FARIDA DEWI
0906651920

FAKULTAS HUKUM
PROGRAM PASCASARJANA
JAKARTA
JUNI 2012

UNIVERSITAS INDONESIA

TANGGUNG JAWAB HUKUM PENYELENGGARA TANDA TANGAN DIGITAL TERSERTIFIKASI YANG BERINDUK (ANALISA KOMPARATIF TERHADAP KASUS DIGINOTAR DI BELANDA)

TESIS

Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Hukum

FARIDA DEWI
0906651920

FAKULTAS HUKUM
PROGRAM PASCASARJANA
JAKARTA
JUNI 2012

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar

Nama : Farida Dewi

NPM : 0906651920

Tanda tangan : 

Tanggal : 28 Juni 2012.

HALAMAN PENGESAHAN

Tesis ini diajukan oleh:

Nama	:	Farida Dewi
NPM	:	0906651920
Program Studi	:	Pascasarjana
Judul Tesis	:	Tanggung Jawab Hukum Penyelenggara Tanda Tangan Digital Tersertifikasi yang Berinduk (Analisa Komparatif terhadap Kasus DigiNotar di Belanda)

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Hukum pada Program Studi Pascasarjana Fakultas Hukum, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing : Dr. Edmon Makarim, S.Kom, S.H., L.L.M. (.....)

Penguji : Prof. Dr. Agus Sardjono S.H., M.H. (.....)

Penguji : Brian Amy Prastyo S.H., MLI (.....)

Ditetapkan di : Depok

Tanggal : 2 Juli 2012

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya sehingga penulis dapat menyelesaikan tesis ini dengan judul "Tanggung Jawab Hukum Penyelenggara Tanda Tangan Digital Tersertifikasi yang Berinduk (Analisa Komparatif terhadap Kasus DigiNotar di Belanda)". Tesis ini disusun untuk memenuhi salah satu syarat guna menyelesaikan studi di Fakultas Hukum Universitas Indonesia agar dapat meraih gelar Magister Hukum (S2).

Dengan tersusunnya tesis ini, penulis menyampaikan ucapan terima kasih kepada semua pihak yang telah membantu dan membimbing penulis hingga tesis ini selesai disusun. Ucapan terima kasih ini disampaikan terutama kepada :

1. Bapak Dr. Edmon Makarim, S.Kom, S.H., LL.M, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, pikiran untuk mengarahkan saya dalam penyusunan tesis ini.
2. Segenap Dosen Pengajar Fakultas Hukum Universitas Indonesia, atas kesabaran dan ketulusan hati dalam mendidik dan memberikan ilmu pengetahuan.
3. Seluruh staf dan pegawai Fakultas Hukum Universitas Indonesia.
4. Keluarga besarku tercinta, khususnya Mak dan Babe yang telah membesarkan, merawat, membimbing dan mencurahkan kasih sayang serta dengan sabar telah mendukung penulis sampai saat ini.
5. Adik kandung penulis, Indah yang dengan tulus memberi semangat, dorongan dan doa sehingga memotivasi penulis menyusun tesis ini.
6. Seluruh saudara sepupu penulis yang tidak dapat disebut satu per satu, yang telah banyak memberi semangat dan memotivasi penulis selama ini.
7. Sahabat-sahabatku di Sunter, yaitu Ade Putra, Felix Wijaya, Irene Surjoprajogo, Nofianti Bundo, Novita Andriany Lorina, Steven Jaya Winartha, San-San Novalia, Stella, Vera Juslim dan Mardecia Paulce yang masih berada di New York, yang senantiasa mendukung, memberikan semangat serta motivasi yang tak henti-hentinya dalam penulisan tesis ini.
8. Teman-teman seperjuangan penulis di Universitas Indonesia, khususnya Nancy Farida, Aluisius Ari, Bapak Sampurno, Kak Dewi Septiani Tarigan,

Bayu Imantoro, Vidya Paramitha serta teman-teman lainnya yang tak dapat disebut satu per satu, yang telah banyak memberikan banyak dukungan kepada penulis selama kuliah hingga rampungnya penyusunan tesis ini.

9. Teman-temanku, yaitu Claudia, Andhika, Aldri, Mariska, Angelina, Fitriana, Agnes, serta teman-teman lainnya yang telah memberikan semangat dan motivasi tak henti-hentinya.
10. Serta seluruh pihak yang tidak dapat penulis sebutkan satu persatu namanya, yang telah memberikan dukungan dan bantuan kepada penulis sehingga memperlancar penulisan tesis ini hingga selesai.

Penulis menyadari bahwa dalam penulisan tesis ini masih terdapat banyak sekali kekurangan. Oleh karena itu saran dan kritik dari pembaca akan sangat berguna bagi penulis. Akhir kata, penulis mengharapkan semoga tesis ini dapat berguna dan bermanfaat bagi semua pihak, serta dapat memberikan informasi dalam perkembangan ilmu hukum.

Jakarta, 28 Juni 2012

Penulis

Farida Dewi

NPM : 0906651920

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan dibawah ini:

Nama : Farida Dewi
NPM : 0906651920
Program Studi : Pascasarjana
Fakultas : Hukum
Jenis Karya : Tesis

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Nonekslusif** (*Non-Exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

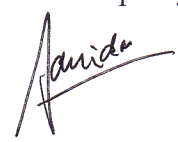
Tanggung Jawab Hukum
Penyelenggara Tanda Tangan Digital Tersertifikasi yang Berinduk
(Analisa Komparatif Terhadap Kasus DigiNotar di Belanda)

Beserta instrumen/desain/perangkat (jika ada). Berdasarkan persetujuan Hak Bebas Royalty Non Eksklusif ini, Universitas Indonesia berhak menyimpan, mengalih bentuk, mengalihmediakan, mengelola dalam bentuk pangkalan data (*database*), merawat serta mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis atau pencipta dan juga sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sesungguhnya secara sadar tanpa paksaan dari pihak manapun.

Dibuat di : Jakarta
Pada tanggal : 28 Juni 2012

Yang membuat pernyataan



(Farida Dewi)

ABSTRAK

Nama : Farida Dewi
Program Studi : Pascasarjana
Judul : Tanggung Jawab Hukum Penyelenggara Tanda Tangan Digital Tersertifikasi yang Berinduk (Analisa Komparatif Terhadap Kasus DigiNotar di Belanda)

Meningkatnya pengguna internet dan juga penetrasi telepon seluler mengakibatkan masyarakat telah melakukan transaksi elektronik. Walau elektronik menghemat banyak waktu dan biaya ketimbang transaksi konvensional, namun transaksi via sistem telekomunikasi konvensional (*circuit switching*) ini relatif lebih aman ketimbang transaksi melalui internet (*packet switching*). Mengingat begitu pentingnya nilai dari sebuah transaksi, maka dalam menjamin keamanan bertransaksi yang dilakukan secara elektronik dapat sama seperti transaksi secara konvensional mengakibatkan munculnya tanda tangan elektronik.

Dengan adanya ketentuan hukum yang mengatur mengenai Tanda Tangan Elektronik (TTE) membawa perubahan besar dalam menjamin autentikasi dan verifikasi serta dengan menghadirkan alat bukti baru pada hukum pembuktian. Nilai kekuatan pembuktian TTE semakin kuat dengan adanya penyelenggara sertifikasi elektronik (*Certificate Authority*/CA) sehingga CA memiliki peran penting dalam menjaga keamanan dari data dan informasi para pihak terkait. Baru-baru ini penyelenggara tanda tangan digital di Belanda, yaitu DigiNotar, mengalami masalah dan menuai tanggung jawabnya sebagai CA. Disisi lain, Indonesia yang telah menggunakan CA asing pada bank-bank Indonesia dan telah tumbuhnya CA asing hendaknya dapat belajar dari kasus DigiNotar tersebut.

Tujuan penelitian ini adalah untuk mengetahui ketentuan hukum TTE dan transaksi elektronik dalam konteks ilmu hukum serta mengkaji dan menganalisis tanggung jawab penyelenggara tanda tangan elektronik di Belanda dan Indonesia dengan menerapkan beberapa faktor dalam ketentuan hukumnya. Penelitian ini menggunakan pendekatan yuridis-empiris, yaitu dengan melakukan inventarisasi hukum positif yang mengatur dan berkaitan dengan TTE dan tanggung jawab CA sedangkan data dalam penelitian ini dianalisis secara kualitatif, yaitu data sekunder yang berupa teori, definisi dan substansinya dari berbagai literatur, dan peraturan perundang-undangan, kemudian dianalisis dengan undang-undang, teori dan pendapat pakar yang relevan, sehingga didapat kesimpulan tentang tanggung jawab hukum penyelenggara tanda tangan elektronik.

Kata kunci : Tanggung Jawab Hukum, Penyelenggara Tanda Tangan, Tanda Tangan Digital, DigiNotar.

ABSTRACT

Name : Farida Dewi
Study Programme : Post Graduate
Title : Law Responsibility for the Main Certificated Digital Signature Vendor (Comparative analysis For DigiNotar case In Netherland)

The increase of Internet users and mobile phone penetration has resulted in the electronic transactions. Although electronic saves a lot of time and cost than conventional transactions, but transactions via conventional telecommunications systems (circuit switching) is relatively more secure than transactions over the Internet (packet switching). To realize the importance of the value of a transaction, Thus to ensuring security of transactions conducted electronically can be the same as in the conventional transaction resulted in the emergence of Digital signatures.

With the legal provisions governing of the Electronic Signatures (e-sign) brought major changes to ensure the authentication and verification as well as by presenting new evidence on the law of evidence. The power value of the e-sign more strength by the organizers of the electronic certification (Certificate Authority / CA) so that CA has an important role in maintaining the security of data and information related parties. Recently, new digital signature providers in the Netherlands, ie: DigiNotar, having problems and reap the responsibility as a CA. On the other hand, Indonesia has used foreign CA on banks in Indonesia and has been the growth of private CA must be able to learn from the case DigiNotar.

The purpose of this study was to determine the legal provisions of e-sign and electronic transactions in the context of legal science as well as review and analyze the responsibility of the electronic signature in the Netherlands and Indonesia by implementing some of the factors in the law. This study uses an empirical approach, juridical, to conduct an inventory of the positive law governing and relating to the e-sign and responsibilities CA while the data in this study were analyzed by qualitatively ie: the secondary data such as theory, the definition and substance of the literature, and legislation and regulations, and then analyzed with the laws, theories and opinions of relevant experts, in order to get conclusions about the legal responsibilities of providers of electronic signatures.

Key words: Law Responsibility, Signature vendor, Digital Signature, DigiNotar

DAFTAR ISI

Bab I
Pendahuluan

1.1. Latar Belakang

Meningkatnya pengguna internet dan juga penetrasi telepon seluler mengakibatkan masyarakat telah melakukan transaksi elektronik. Transaksi elektronik bertitik tolak pada kemudahan pemberian informasi yang diberikan internet. Internet (*interconnection networking*) merupakan implementasi *Transmission Control Protocol/Internet Protocol* (TCP/IP) yang telah memberikan kemudahan dalam berkomunikasi secara global tanpa batasan geografis antar negara termasuk melakukan transaksi bisnis antarnegara.[1]

Tak dapat dipungkiri bahwa perkembangan dalam internet mempermudah terpenuhinya kebutuhan dalam kehidupan masyarakat sehingga membuat berbagai aspek kehidupan berjalan semakin dinamis. Seperti halnya kemampuan dalam bertransaksi melalui internet dapat dilakukan secara efisien dan efektif. Para pihak yang bertransaksi tidak perlu bertatap muka seperti layaknya transaksi secara konvensional sehingga dapat menghemat waktu dan biaya. Walau transaksi konvensional menyita banyak waktu dan biaya dalam segi efisiensi, namun transaksi via sistem telekomunikasi konvensional (*circuit switching*) ini relatif lebih aman ketimbang transaksi melalui internet (*packet switching*). Mengingat begitu pentingnya nilai dari sebuah transaksi, maka dalam menjamin keamanan bertransaksi yang dilakukan secara elektronik dapat sama seperti transaksi secara konvensional mengakibatkan munculnya tanda tangan elektronik.

Keamanan dalam bertransaksi atau pertukaran informasi merupakan aspek penting yang harus diperhatikan dari sebuah sistem informasi atau sistem bertransaksi. Sayangnya permasalahan keamanan informasi ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Tidak jarang masalah keamanan berada di urutan kedua atau bahkan di urutan

[1] Yahya Ahmad Zein, *Kontrak Elektronik & Penyelesaian Sengketa Bisnis E-Commerce*. (Bandung: Mandar Maju, 2009), hlm.3.

terakhir dalam daftar hal-hal yang dianggap penting. Meskipun sering terlihat sebagai besaran yang tidak dapat langsung diukur dengan uang (*intangible*), keamanan sebuah sistem informasi sebetulnya dapat diukur dengan besaran yang dapat diukur dengan uang (*tangible*).[2] Berikut ini adalah berapa contoh perkiraan kegiatan yang diukur baik langsung dengan uang maupun yang tidak dapat diukur langsung dengan uang:[3]

a. Hitung kerugian apabila sistem informasi tidak bekerja selama 1 jam, selama 1 hari, 1 minggu, dan 1 bulan. (Sebagai perbandingkan, bayangkan jika server Amazon.com tidak dapat diakses selama beberapa hari. Setiap harinya server tersebut dapat menderita kerugian beberapa juta dolar.)
b. Hitung kerugian apabila ada kesalahan informasi (data) pada sistem informasi. Misalnya sebuah *website* mengumumkan harga sebuah barang yang berbeda dengan harga yang ada di toko dari *website* tersebut.
c. Hitung kerugian apabila ada data yang hilang, misalnya berapa kerugian yang diderita apabila daftar pelanggan dan *invoice* hilang dari sistem. Berapa biaya yang dibutuhkan untuk rekonstruksi data.
d. Apakah nama baik perusahaan/individu merupakan sebuah hal yang harus dilindungi? Bayangkan bila sebuah bank terkenal dengan rentannya pengamanan data-datanya, bolak-balik terjadi *security incidents*. Tentunya banyak nasabah yang pindah ke bank lain karena takut akan keamanan uangnya.

Apabila sistem informasi tidak bekerja dengan baik seperti yang dipaparkan di atas, maka permasalahan yang mucul dapat dibagi ke dalam dua bagian:[4]

1. Permasalahan yang sifatnya substantif, yakni:
   a. Keaslian *data message* dan tanda tangan elektronik. Masalah keotentikan *data message* ini menjadi permasalahan yang sangat vital

[2] *http://fairuzelsaid.wordpress.com/2010/08/24/cyberlaw-konsep-keamanan-sistem-informasi/*
[3] *Ibid.*
[4] Ridwan Khairandy. *Pengakuan dan Keabsahan Digital Signature dalam Perspektif Hukum Pembuktian.* Jurnal hukum vol.18, Maret 2002, Hlm.31.

dalam *e-commerce*, karena *data message* inilah yang dijadikan dasar utama terciptanya suatu kontrak, baik itu dalam hubungannya dengan kesepakatan ketentuan-ketentuan dan persyaratan kontrak ataupun dengan substansi kesepakatan itu sendiri;

b. Keabsahan (*validity*). Keabsahan suatu kontrak tergantung pada pemenuhan syarat-syarat kontrak telah terpenuhi, utamanya adalah adanya kesepakatan atau persetujuan antara para pihak, maka kontrak dinyatakan terjadi. Dalam *e-commerce* ini, terjadinya kesepakatan sangat erat hubungannya dengan penerimaan atas absah dan otentiknya *data message* yang memuat kesepakatan itu.
c. Kerahasiaan (*confidentiality/privacy*). Kerahasiaan yang dimaksud meliputi kerahasiaan data dan/atau informasi dan juga perlindungan terhadap data dan informasi dan juga perlindungan terhadap data dan informasi dan juga perlindungan terhadap data dan informasi tersebut dari akses yang tidak sah dan berwenang.
d. Keamanan (*security*). Masalah keamanan merupakan masalah penting karena keberadaannya menciptakan rasa *confidence* bagi para *user* dan pelaku bisnis untuk tetap menggunakan media elektronik untuk kepentingan bisnisnya.
e. Ketersediaan (*availability*). Permasalahan lain yang juga harus diperhatikan adalah keberadaan informasi yang dibuat dan ditransmisikan secara elektronik yang harus tersedia setiap kali dibutuhkan.

2. Permasalahan yang bersifat prosedural, yakni:

   Pengakuan dan daya mengikat putusan hakim suatu negara lain untuk diberlakukan dan dilaksanakan negara lawan, sekalipun hal ini memakai instrumen-instrumen internasional, seperti konvensi Brussel, Lugano yang memberikan contoh *jurisdiction exorbitant*, menjadi suatu permasalahan yang cukup kompleks, terutama dalam hubungannya dengan aplikasi *e-commerce.*

Menjawab permasalahan, maka munculnya tanda tangan elektronik membawa dampak besar dalam menjamin keamanan bertransaksi secara elektronik. Dengan dikeluarkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian disahkan pada tanggal 21 April 2008, banyak perubahan yang telah terjadi. Selain dokumen atau informasi elektronik yang ditandatangani dengan sebuah tandatangan elektronik hadir sebagai alat bukti lain sesuai hukum acara yang berlaku, pada pasal 11 UU ITE mengatur pula mengenai tanda tangan elektronik sebagai salah satu alat verifikasi dalam meningkatkan sistem pengamanan dan berperan sebagai alat bukti dalam bertransaksi melalui jaringan internet. UU ITE ini telah membuat perubahan yang besar bagi alat pembuktian yang sebelumnya tidak memasukkan unsur internet.

Walau tak dapat dipungkiri seseorang yang menerapkan tingkat keamanan tertentu akan mendapati kebebasannya berkurang sesuai tingkat keamanan yang diberlakukan. Sesuai dengan kebalikannya, semakin bebas maka keamanannya semakin berkurang dengan adanya pemberian identitas dan lain sebagainya. Seperti halnya dalam memperkuat legalitas pada transaksi elektronik yang semakin marak pada saat ini terkadang membutuhkan suatu informasi atau data yang harus diserahkan pada pihak lain sehingga tingkat keamanan data atau informasi menjadi peringkat utama yang seharusnya diperhatikan dalam rangka mencegah penyalahgunaan data atau informasi tersebut. Oleh karena itu, sistem pengamanan haruslah dirancang sedemikian rupa sehingga tidak ada celah bagi yang tidak bertanggung jawab dalam menyalahgunakan data atau informasi tersebut.

Dengan demikian, seperti yang telah dijabarkan sebelumnya, diperlukanlah tanda tangan elektronik di dalam transaksi elektronik yang bertujuan sebagai alat verifikasi dan otentikasi. Dalam memperkuat tujuan dari tanda tangan elektronik diperlukan pula keterlibatan pihak ketiga, dalam hal ini keterlibatan penyelenggara tanda tangan elektronik itu sendiri. Dengan adanya keikutsertaan penyelenggara tanda tangan elektronik, data atau informasi elektronik yang terkait semakin kuat dan sulit dibantah validitasnya. Namun,

tidak semua rencana berjalan sesuai dengan harapan, adanya ancaman-ancaman dari luar (*hacking*, *virus*, dan lain sebagainya) serta sistem pengamanan yang tidak ter-*update* serta sistem yang tidak dikontrol dengan baik dapat mengakibatkan penyelenggara tanda tangan elektronik sebagai penguat dalam transaksi elektronik pun dibobol.

Baru-baru ini penyelenggara tanda tangan digital di Belanda, yaitu DigiNotar mengalami masalah dan menuai tanggung jawab hukumnya. Sebagai penyelenggara tanda tangan digital, DigiNotar memikul tanggung jawab terhadap para klien atau konsumennya sehingga diperlukan sistem pengamanan yang ekstra ketat dalam menjaga data atau informasi para konsumennya. Sayangnya, dengan adanya kasus peretasan yang terjadi pada DigiNotar sehingga dapat dikatakan bahwa DigiNotar tidak berhasil melindungi informasi yang telah diberikan padanya. Hal ini akan relevan dengan Indonesia yang telah menggunakan CA asing pada bank-bank di Indonesia dan tumbuhnya CA swasta.

Berdasarkan permasalahan ini, maka dapat ditarik kesimpulan bahwa dengan hadirnya transaksi yang menggunakan via internet ini relatif kurang aman bila dibandingkan dengan transaksi secara konvensional. Sehingga transaksi elektronik ini menuntut adanya perlindungan baik dari segi teknologi maupun dari segi yuridiksi. Perlindungan dari segi teknologi yang sekiranya mampu memberikan keamanan dengan menggunakan teknik kriptografi pada tanda tangan elektronik sedangkan dalam menjamin keamanan segi yuridiksi terdapat pada pasal 11 UU ITE dibahas mengenai tandatangan elektronik dimana dinyatakan pengakuan secara tegas bahwa meskipun sebuah kode, namun tandatangan elektronik memiliki kekuatan hukum yang sama dengan tanda tangan secara manual pada umumnya sehingga keamanan dan pembuktian dalam berniaga lebih terjamin. Ditambah lagi dengan adanya keterlibatan penyelenggara tanda tangan elektronik yang memperkuat kebenaran dan validitas data atau informasi elektronik sehingga menimbulkan tanggung jawab hukum penyelenggara tersebut. Sayangnya perkembangan teknologi serta produk hukum ini tidak sepenuhnya berjalan dengan dinamika masyarakat

Indonesia dalam merumuskan suatu kebijakan sehingga masyarakat seolah tampak terlambat dalam mengiringi perkembangan teknologi tersebut. Berdasarkan latar belakang masalah tersebut, maka penulis ingin meneliti dan menyusun tesis yang berjudul : **"TANGGUNG JAWAB HUKUM PENYELENGGARA TANDA TANGAN DIGITAL TERSERTIFIKASI YANG BERINDUK (ANALISA KOMPARATIF TERHADAP KASUS DIGINOTAR DI BELANDA)."**

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka terdapat beberapa rumusan masalah yang ingin diteliti, yakni:

1. Bagaimanakah ketentuan hukum yang mengatur tentang tanda tangan elektronik dan transaksi elektronik?
2. Bagaimanakah tanggung jawab hukum penyelenggara tanda tangan elektronik, khususnya dengan memperhatikan kasus DigiNotar di Belanda?

1.3. Tujuan Penelitian

1. Untuk mengetahui ketentuan hukum mengenai tanda tangan elektronik dan transaksi elektronik.
2. Untuk mengetahui tanggung jawab hukum hukum penyelenggara tanda tangan elektronik, khususnya terkait dengan kasus yang terjadi pada DigiNotar di Belanda.

1.4. Metode Penelitian

Metode penelitian ini dikelompokan menjadi 5 (lima) bagian, yaitu:

1. Metode Pendekatan

   Penelitian ini menggunakan pendekatan *yuridis normatif*, yaitu dengan melakukan analisis hukum positif yang mengatur berkaitan antara tanda tangan elektronik dan transaksi elektronik, pengaturannya dalam KUHPerdata maupun peraturan perundang-undangan terkait lainnya,

menganalisa keamanan informasi dan kekuatan pembuktiannya serta tanggung jawab hukum penyelenggara tanda tangan elektronik khususnya penyelenggara tanda tangan digital tersertifikasi yang berinduk beserta analisis terhadap kasus DigiNotar di Belanda.

2. Spesifikasi Penelitian

   Penelitian ini merupakan penelitian secara *prespektif-analitis* dengan jalan menggambarkan secara rinci, sistematik, dan menyeluruh mengenai segala hal yang berhubungan dengan penyelenggara tanda tangan elektronik. Kemudian dilakukan analisis terhadap aspek hukum pengaturannya di dalam KUHPerdata maupun peraturan perundang-undangan terkait lainnya, menganalisa fungsi dan kekuatan penggunaannya serta kendala-kendala yang dihadapi.

3. Sumber dan Jenis Data

   Sumber data yang dibutuhkan meliputi data sekunder yang diperoleh dari bahan hukum primer dan bahan hukum sekunder. Data sekunder yang diteliti adalah sebagai berikut:

   (a) *Bahan hukum primer* adalah bahan yang isinya mengikat karena dikeluarkan oleh pemerintah atau negara, antara lain meliputi peraturan perundang-undangan, keputusan pengadilan, dan traktat.

   (b) *Bahan hukum sekunder*, yaitu bahan yang memberikan penjelasan tentang bahan hukum primer, yaitu berupa dokumen atau risalah perundang-undangan.

   (c) *Bahan hukum tersier*, yang memberikan penjelasan lebih mendalam mengenai bahan hukum primer maupun bahan hukum sekunder disebut bahan referensi, bahan acuan, atau rujukan,[5] antara lain: Kamus Hukum, Koran, Majalah, Jurnal Hukum, Artikel Hukum.

4. Teknik Pengumpulan Data

   Untuk memperoleh data digunakan teknik pengumpulan data dengan studi dokumen/kepustakaan.

[5] Burhan Ashshofa, *Metode Penelitian Hukum,* (Jakarta: Rineka Cipta, 1998), hlm. 103-104.

5. Metode Analisa Data

   Data dalam penelitian ini dianalisis secara *kualitatif*,[6] yaitu data sekunder yang berupa teori, definisi, dan substansinya dari berbagai literatur, dan peraturan perundang-undangan, kemudian dianalisis dengan undang-undang, teori dan pendapat pakar yang relevan serta disusun sesuai dengan tujuan penelitian.

1.5. Kerangka Teori

Dalam dunia ilmu, teori menempati kedudukan yang penting sebagai sarana untuk merangkum serta memahami permasalahan secara lebih baik. Teori memberikan penjelasan melalui cara mengorganisasikan dan mensistematiskan masalah yang dibahas.

Teori yang akan digunakan adalah teori *secured communication*. Teori ini merupakan teori yang membahas mengenai beberapa prinsip sistem komunikasi yang aman. Prinsip tersebut meliputi *Confidentiality, Integrity, Authorization, Availability, Authenticity, Non-Repudiation,* dan *Auditability* (CIAANA). Adapun penjelasannya mengenai aspek pengamanan tersebut sebagai berikut:

1. *Confidentiality*[7]

   Inti utama aspek *confidentiality* atau dapat juga disebut dengan *privacy* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Privacy* lebih ke arah data-data yang sifatnya privat sedangkan *confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

   Confidentiality merupakan aspek yang menyangkut kerahasiaan data dan/atau informasi, dimana perlindungan informasi tersebut dilindungi dari pihak yang tidak berwenang. Caranya adalah dengan

[6] Soerjono Soekanto, *Pengantar Penelitian Hukum*, (Penerbit UI Press, 2006), hlm. 250.
[7] Fairuz. *Op.Cit.*

membuat informasi itu "tidak dapat dipahami" (*unintelligible*) oleh pihak-pihak yang tidak berwenang atau tidak bertanggung jawab itu. Untuk membuat informasi itu "tidak dapat dipahami", isi dari informasi itu harus ditransformasikan sedemikian rupa sehingga tidak dapat dipahami (tidak *decipherable*) oleh siapapun yang tidak mengetahui prosedur proses transformasi itu.

Contoh hal yang berhubungan dengan *privacy* adalah *e-mail* seorang pemakai tidak boleh dibaca oleh administrator. Contoh *confidential information* adalah data-data yang sifatnya pribadi seperti nama, tempat tanggal lahir, *social security number*, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya merupakan data-data yang ingin diproteksi penggunaan dan penyebarannya. Contoh lain dari *confidentiality* adalah daftar pelanggan dari sebuah *Internet Service Provider* (ISP).

2. *Integrity*

Integrity menyangkut perlindungan data terhadap usaha memodifikasikan data itu oleh pihak-pihak yang tidak bertanggung jawab, baik selama data itu disimpan atau selama data itu dikirimkan kepada pihak lain. Sistem pengamanan harus mampu memastikan bahwa pada waktu diterima oleh penerima, informasi itu harus muncul sama seperti ketika informasi itu disimpan atau dikirimkan. Sistem pengamanan yang dibangun harus memungkinkan untuk mengetahui apabila isi asli dari informasi yang dikirimkan itu telah terjadi modifikasi, tambahan, atau penghapusan. Sistem tersebut juga harus dapat mencegah "dimainkannya kembali" (*re-played*) informasi itu, misalnya *fresh copy* dari data tersebut dikirimkan lagi dengan menggunakan otorisasi yang semula dipakai ketika pesan yang sesungguhnya itu dikirimkan. Oleh karena itu, diperlukan adanya suatu mekanisme yang dapat memastikan kebenaran isi pesan yang dikirimkan itu dan untuk dapat memastikan otentikasi atas pembuatan salinan dari pesan tersebut, yaitu otentikasi bahwa salinan itu sesuai dengan aslinya.

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah *e-mail* dapat saja "ditangkap" di tengah jalan, diubah isinya kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Dalam mengatasi masalah ini, salah satu caranya dengan dilakukannya penggunaan enkripsi dan *digital signature*.

Salah satu contoh kasus adalah *trojan horse* dengan distribusi paket program TCP *Wrapper* (yaitu program populer yang dapat digunakan untuk mengatur dan membatasi akses TCP/IP) yang dimodifikasi oleh orang yang tidak bertanggung jawab. Jika memasang program yang berisi *trojan horse*, maka saat merakit (*compile*) program tersebut, dia akan mengirimkan *e-mail* kepada orang tertentu yang kemudian memperbolehkan dia masuk ke sistem yang berisi program tersebut. Contoh serangan lain adalah yang disebut "*man in the middle attack"* dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

3. *Authenticity*[8]

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli. Semua pihak yang terlibat harus merasa aman bahwa komunikasi yang terjadi melalui jaringan di antara pihak-pihak itu adalah benar, yaitu benar bahwa para pihak berhubungan dengan pihak-pihak yang sesungguhnya diinginkan dan benar mengenai informasi yang dipertukarkan di antara mereka. Apabila suatu pesan diterima, maka penerima harus dapat memverifikasi bahwa pesan itu benar-benar dikirimkan oleh orang atau pihak yang sesungguhnya. Sebaliknya juga, harus dapat dipastikan bahwa pesan

[8] *Ibid.*

tersebut memang telah dikirimkan kepada dan telah diterima oleh pihak yang sesungguhnya dituju.

Permasalahan pertama dalam membuktikan keaslian dokumen dapat dilakukan dengan teknologi *watermarking* dan *digital signature. Watermarking* juga dapat digunakan untuk menjaga *intelectual property,* yaitu dengan menandai dokumen atau hasil karya dengan tanda tangan pembuat. Permasalahan kedua biasanya berhubungan dengan *access control,* yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi.

Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan *password, biometric* (ciri-ciri khas orang), dan sejenisnya. Ada tiga hal yang dapat ditanyakan kepada orang untuk menguji siapa dia:

a. *What you have* (misalnya kartu ATM),
b. *What you know* (misalnya PIN atau *password*), dan
c. *What you are* (misalnya sidik jari, *biometric*)

Penggunaan teknologi *smart card* saat ini kelihatannya dapat meningkatkan keamanan dalam prinsip ini. Secara umum, proteksi *authentication* dapat menggunakan *digital certificates*.

Authenticity biasanya diarahkan kepada orang (pengguna), namun tidak pernah ditujukan kepada server atau mesin. Pernahkan kita bertanya bahwa mesin ATM yang sedang kita gunakan memang benar-benar milik bank yang bersangkutan? Bagaimana jika ada orang yang tidak bertanggung jawab yang membuat mesin seperti ATM sebuah bank dan meletakkannya di tempat umum? Orang tersebut dapat menyadap data-data (informasi yang ada di *magnetic strip*) dan PIN dari orang yang tertipu. Walau membuat mesin ATM palsu tidak mudah, namun dapat di bayangkan betapa mudahnya membuat *website* palsu dengan menyamar sebagai web site sebuah bank yang memberikan layanan *Internet Banking*. (Ini yang terjadi dengan kasus klikBCA.com.)

4. *Authorization*[9]

Authorization menyangkut pengawasan terhadap akses kepada informasi tertentu. Transaksi-transaksi tertentu mungkin hanya dapat diakses oleh pihak-pihak tertentu saja, sedangkan transaksi-transaksi yang lain tidak. *Authorization* dimaksudkan untuk membatasi perbuatan oleh pihak-pihak yang tidak berwenang untuk dapat berbuat sesuatu di dalam lingkungan jaringan informasi itu. Pembatasan tersebut tergantung pada *security level* dari pihak yang bersangkutan.

Pembatasan itu menyangkut sampai sejauh mana pihak yang diberi kewenangan untuk melakukan akses terhadap hal itu diberi wewenang untuk dapat melakukan hal-hal sebagai berikut:

a. Memasukan data/informasi,
b. Membaca data/informasi,
c. Memodifikasi, menambah, atau menghapus data/informasi,
d. Mengekspor atau mengimpor data/informasi, dan
e. Menge-*print* data/informasi.

Hak-hak istimewa tersebut dapat dikendalikan atau diawasi baik oleh petugas tertentu atau oleh suatu unit tertentu yang ditugasi khusus untuk keperluan tersebut, dengan cara menggunakan *access control list* (ACL). ACL adalah suatu daftar yang memuat siapa saja dan tingkat kewenangan dari masing-masing orang atau pejabat tersebut untuk mengakses data itu.

5. *Non-repudiation*

Aspek ini dikenal dengan *non-repudiation of origin* atau *non-repudiability* atau disebut juga *non-repudiation,* dimana aspek ini berperan dalam melindungi atau menjaga agar seseorang tidak dapat menyangkal bahwa telah terjadi sebuah transaksi atau kegiatan komunikasi yang memang benar telah terjadi. Aspek ini harus dapat

[9] Sutan Remy Sjahdeini, *Sistem Pengamanan E-Commerce*, Jurnal hukum bisnis vol.18, 2002, Hlm.6.

membuktikan kepada pihak ketiga yang independen mengenai originalitas dan mengenai pengiriman data yang dipersoalkan itu.

Sebagai contoh, seseorang yang mengirimkan *e-mail* untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut. Prinsip ini sangat penting dalam hal melakukan *electronic commerce*. Penggunaan *digital signature, certificates* dan teknologi kriptografi secara umum dapat menjaga prinsip ini. Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari *digital signature* itu jelas legal.

6. *Availability*[10]

Prinsip *availability* berhubungan dengan ketersediaan informasi ketika dibutuhkan atau saat hendak diakses. Informasi yang disimpan atau ditransmisikan melalui jaringan komunikasi harus dapat tersedia sewaktu-waktu apabila diperlukan. Sistem perlindungan itu harus dapat mencegah timbulnya sebab-sebab yang dapat menghalangi tersedianya informasi yang diperlukan itu. Kesalahan-kesalahan jaringan (*network errors*), listrik mati (*power outages*), kesalahan-kesalahan operasional (*operational errors*), kesalahan-kesalahan yang bersangkutan dengan aplikasi peranti lunak yang digunakan (*software application*), masalah-masalah yang menyangkut peranti keras (*hardware problems*), dan virus merupakan beberapa sebab yang dapat membuat informasi yang diperlukan itu menjadi tidak tersedia ketika dibutuhkan (*unavailability of information*).

Sebagai contoh, serangan yang sering disebut dengan "*denial of service attack" (DoS attack)*, dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down, hang, crash*. Contoh lain adalah adanya *mailbomb*, dimana seorang pemakai dikirimi *e-mail* bertubi-tubi dengan ukuran yang besar sehingga

[10] *Ibid.*

sang pemakai tidak dapat membuka *e-mail*nya atau kesulitan mengakses *e-mail*nya.

7. *Auditablity*[11]

Data tersebut harus dicatat sedemikian rupa bahwa terhadap data itu semua syarat-syarat *confidentiality* dan *integrity* yang diperlukan telah terpenuhi, yaitu bahwa pengiriman data tersebut telah dienkripsi (*encrypted*) oleh pengirimnya dan telah didekripsi (*decrypted*) oleh penerimanya sebagaimana mestinya.

Teori selanjutnya adalah teori pertanggungjawaban. Ada dua istilah yang menunjuk pada pertanggungjawaban dalam kamus hukum, yaitu *liability* dan *responsibility*. *Liability* merupakan istilah hukum yang luas yang menunjuk hampir semua karakter risiko atau tanggung jawab, yang pasti, yang bergantung atau yang mungkin meliputi semua karakter hak dan kewajiban secara aktual atau potensial seperti kerugian, ancaman, kejahatan, biaya atau kondisi yang menciptakan tugas untuk melaksanakan undang-undang. *Responsibility* berarti hal yang dapat dipertanggungjawabkan atas suatu kewajiban, dan termasuk putusan, ketrampilan, kemampuan dan kecakapan meliputi juga kewajiban bertanggung jawab atas undang-undang yang dilaksanakan. Dalam pengertian dan penggunaan praktis, istilah *liability* menunjuk pada pertanggungjawaban hukum, yaitu tanggung gugat akibat kesalahan yang dilakukan oleh subyek hukum, sedangkan istilah *responsibility* menunjuk pada pertanggungjawaban politik.[12]

Mengenai persoalan pertanggungjawaban pejabat menurut Kranenburg dan Vegtig ada dua teori yang melandasinya yaitu:

a. Teori *fautes personalles*, yaitu teori yang menyatakan bahwa kerugian terhadap pihak ketiga dibebankan kepada pejabat yang karena tindakannya itu telah menimbulkan kerugian. Dalam teori ini beban tanggung jawab ditujukan pada manusia selaku pribadi.

[11] *Ibid.*

[12] Ridwan H.R., *Hukum Administrasi Negara*, Raja Grafindo Persada, Jakarta, 2006, hlm. 335-337.

b. Teori *fautes de services*, yaitu teori yang menyatakan bahwa kerugian terhadap pihak ketiga dibebankan pada instansi dari pejabat yang bersangkutan. Menurut teori ini tanggung jawab dibebankan kepada jabatan. Dalam penerapannya, kerugian yang timbul itu disesuaikan pula apakah kesalahan yang dilakukan itu merupakan kesalahan berat atau kesalahan ringan, dimana berat dan ringannya suatu kesalahan berimplikasi pada tanggung jawab yang harus ditanggung.[13]

Secara umum prinsip-prinsip tanggung jawab dalam hukum dapat dibedakan sebagai berikut:[14]

1) Prinsip Tanggung Jawab Berdasarkan Unsur Kesalahan

Prinsip tanggung jawab berdasarkan unsur kesalahan (*fault liability* atau *liability based on fault*) adalah prinsip yang cukup umum berlaku dalam hukum pidana dan perdata. Dalam Kitab Undang-Undang Hukum Perdata, khususnya diatur di dalam pasal 1365, 1366, dan 1367. Prinsip ini menyatakan bahwa seseorang baru dapat dimintakan pertanggungjawabannya secara hukum jika ada unsur kesalahan yang dilakukannya.

Pasal 1365 Kitab Undang-Undang Hukum Perdata yang lazim dikenal sebagai pasal tentang perbuatan melawan hukum, mengharuskan terpenuhinya empat unsur pokok, yaitu:

a. adanya perbuatan,
b. adanya unsur kesalahan,
c. adanya kerugian yang diderita,
d. adanya hubungan kausalitas antara kesalahan dan kerugian.

Yang dimaksud kesalahan adalah unsur yang bertentangan dengan hukum. Pengertian hukum tidak hanya bertentangan dengan undang-undang tetapi juga kepatutan dan kesusilaan dalam masyarakat.

[13] *Ibid.*, hlm. 365.
[14] Shidarta, *Hukum Perlindungan Konsumen Indonesia, Edisi Revisi*, Gramedia Widiasarana Indonesia, Jakarta, 2006, hlm. 73-79.

2) Prinsip Praduga Untuk Selalu Bertanggung Jawab

Prinsip ini menyatakan bahwa tergugat selalu dianggap bertanggung jawab (*presumption of liability principl*e) sampai ia dapat membuktikan bahwa ia tidak bersalah. Kata "dianggap" pada prinsip *presumption of liability* adalah penting, karena ada kemungkinan tergugat membebaskan diri dari tanggung jawab, yaitu dalam hal ia dapat membuktikan bahwa ia telah mengambil semua tindakan yang diperlukan untuk menghindarkan terjadinya kerugian.[15]

Dalam prinsip ini, beban pembuktiannya ada pada si tergugat. Dalam hal ini tampak beban pembuktian terbalik (*omkering van bewijslast*). Hal ini tentu bertentangan dengan asas hukum praduga tidak bersalah (*presumption of innocence*). Namun jika diterapkan dalam kasus konsumen akan tampak asas demikian cukup relevan. Jika digunakan teori ini, maka yang berkewajiban untuk membuktikan kesalahan itu ada pada pihak pelaku usaha yang digugat. Tergugat harus menghadirkan bukti-bukti bahwa dirinya tidak bersalah. Tentu saja konsumen tidak dapat sekehendak hati mengajukan gugatan. Posisi konsumen sebagai penggugat selalu terbuka untuk digugat balik oleh pelaku usaha, jika ia gagal menunjukkan kesalahan tergugat.

3) Prinsip Praduga Untuk Tidak Selalu Bertanggung Jawab

Prinsip ini adalah kebalikan dari prinsip yang kedua, prinsip praduga untuk tidak selalu bertanggung jawab hanya dikenal dalam lingkup transaksi konsumen yang sangat terbatas. Contoh dari penerapan prinsip ini adalah pada hukum pengangkutan. Kehilangan atau kerusakan pada bagasi kabin atau bagasi tangan, yang biasanya dibawa dan diawasi oleh penumpang (konsumen) adalah tanggung jawab dari penumpang. Dalam hal ini pengangkut (pelaku usaha) tidak dapat dimintakan

[15] E. Suherman, *Masalah Tanggung Jawab Pada Charter Pesawat Udara Dan Beberapa Masalah Lain Dalam Bidang Penerbangan (Kumpulan Karangan),* Cet. II, Alumni, Bandung, 1979, hlm. 21.

pertanggungjawabannya. Pihak yang dibebankan untuk membuktikan kesalahan itu ada pada konsumen.

4) Prinsip Tanggung Jawab Mutlak (Absolut)

Prinsip ini menetapkan bahwa suatu tindakan dapat dihukum atas dasar perilaku berbahaya yang merugikan (*harmful conduct*) tanpa mempersoalkan ada tidaknya kesengajaan (*intention*) atau kelalaian (*negligence*). Prinsip ini menegaskan hubungan kausalitas antara subyek yang bertanggung jawab dan kesalahan dibuatnya, dengan memperhatikan adanya *force majeur* sebagai faktor yang dapat melepaskan diri dari tanggung jawab.

5) Prinsip Tanggung Jawab Dengan Pembatasan

Prinsip tanggung jawab dengan pembatasan (*limitation of liability principle*) ini sangat disenangi oleh pelaku usaha untuk dicantumkan sebagai klausula eksonerasi dalam perjanjian standar yang dibuatnya. Dalam perjanjian cuci cetak film, misalnya ditentukan, bila film yang ingin dicuci atau dicetak itu hilang atau rusak (termasuk akibat kesalahan petugas), maka si konsumen hanya dibatasi ganti kerugian sebesar sepuluh kali harga satu rol film baru.

Dalam ketentuan pasal 19 ayat 1 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK) ditentukan bahwa pelaku usaha bertanggung jawab memberikan ganti kerugian atas kerusakan, pencemaran dan/atau kerugian konsumen akibat mengkonsumsi barang dan/atau jasa yang dihasilkan. Dalam kaitan dengan pelaksanaan jabatan notaris maka diperlukan tanggung jawab profesional berhubungan dengan jasa yang diberikan. Menurut Komar Kantaatmaja sebagaimana dikutip oleh Shidarta menyatakan tanggung jawab profesional adalah tanggung jawab hukum (*legal liability*) dalam hubungan dengan jasa profesional yang diberikan kepada klien. Tanggung jawab profesional ini dapat timbul karena mereka (para penyedia jasa profesional) tidak memenuhi perjanjian yang mereka sepakati dengan klien mereka atau

akibat dari kelalaian penyedia jasa tersebut mengakibatkan terjadinya perbuatan melawan hukum.[16]

Teori selanjutnya adalah teori keadilan interaktif (*interactive justice*) oleh Edmon Makarim dalam bukunya yang berjudul Tanggung Jawab Hukum Penyelenggara Sistem Elektronik. Teori keadilan interaktif merupakan teori hukum tentang adanya suatu kewajiban hukum atau pertanggungjawaban hukum (*legal responsibilities*) terhadap setiap tindakan interaktif antara manusia.[17] Dengan kata lain, suatu tanggung jawab setiap orang kepada orang lain adalah sebagai konsekuensi hukum adanya penghargaan yang sama terhadap kebebasan eksternal setiap orang (*right to equal external freedom*).[18]

Tanggung jawab (*responsibility*) merupakan suatu refleksi tingkah laku manusia. Penampilan tingkah laku manusia terkait dengan kontrol jiwanya, merupakan bagian dari bentuk pertimbangan intelektualnya atau mentalnya. Bilamana suatu keputusan telah diambil atau ditolak, sudah merupakan bagian dari tanggung jawab dan akibat pilihannya. Tidak ada alasan lain mengapa hal itu dilakukan atau ditinggalkan. Keputusan tersebut dianggap telah dipimpin oleh kesadaran intelektualnya.[19]

1.6. Definisi Operasional

Tanda Tangan Elektronik adalah tanda tangan yang terdiri dari atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.[20]

Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.[21]

---

[16] Shidarta, *Op.Cit.*, Hlm.79.

[17] Edmon Marakim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik.* PR Rajagrafindo Persada, Jakarta, 2010. Hlm.14.

[18] *Ibid.*

[19] Masyhur Efendi, *Dimensi / Dinamika Hak Asasi Manusia Dalam Hukum Nasional Dan Internasional*, Ghalia Indonesia, Jakarta, 1994, hlm. 121.

[20] Indonesia, Undang-Undang Tentang Informasi dan Transaksi Elektronik. UU No.11/2008, LN. No. 58 Tahun 2008, Pasal 1 angka (12).

Pelaku Usaha adalah setiap orang perorangan atau badan usaha, baik yang berbentuk berbadan hukum maupun bukan badan hukum yang didirikan dan berkedudukan atau melakukan kegiatan usaha dalam wilayah hukum Negara Republik Indonesia, baik sendiri maupun bersama-sama melalui perjanjian menyelenggarakan kegiatan usaha dalam berbagai bidang ekonomi.[22]

Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (*EDI*), surat elektronik (*electronic mail)*, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.[23]

Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.[24]

Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.[25]

Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum

---

[21] *Ibid*, Pasal 1 angka (2).

[22] Indonesia, Undang-Undang Tentang Perlindungan Konsumen. UU No.5/1999, LN. No. 42 Tahun 1999, Pasal 1 angka (3).

[23] Indonesia, Undang-Undang Tentang Informasi dan Transaksi Elektronik. UU No.11/2008, LN. No. 58 Tahun 2008, Pasal 1 angka (1).

[24] *Ibid*, Pasal 1 angka (5).

[25] *Ibid*, Pasal 1 angka (6).

para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.[26]

Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.[27]

Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam Transaksi Elektronik.[28]

Penanda Tangan adalah subjek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik.[29]

Kontrak Elektronik adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik.[30]

1.7. Sistematika Penulisan

Hasil penelitian ini akan disusun sebagai tesis dengan sistematika penulisan sebagai berikut:

Dalam BAB I sebagai pendahuluan yang memuat latar belakang, rumusan masalah, tujuan penelitian, metode penelitian, kerangka teori, definisi operasional, dan diakhiri dengan sistematika penulisan.

Pada BAB II akan membahas mengenai ketentuan hukum tanda tangan elektronik dan transaksi elektronik yang mencakup 5 (lima) subbab, yaitu komunikasi elektronik dan transaksi elektronik, tanda tangan elektronik dan

[26] *Ibid*, Pasal 1 angka (9).
[27] *Ibid*, Pasal 1 angka (10).
[28] *Ibid*, Pasal 1 angka (11).
[29] *Ibid*, Pasal 1 angka (13).
[30] *Ibid*, Pasal 1 angka (17).

sertifikasi elektronik, regulasi kriptografi dan standar keamanan informasi serta yang terakhir subbab mengenai informasi sebagai alat bukti.

Selanjutnya pada BAB III akan membahas mengenai tanggung jawab hukum penyelenggara tanda tangan elektronik yang mencakup 3 (tiga) subbab, yaitu tanggung jawab hukum penyelenggara sistem elektronik, tanggung jawab pelaku usaha terhadap konsumen dan analisis tanggung jawab hukum pada kasus DigiNotar di Belanda. Adapun tanggung jawab dalam bab ini meliputi tanggung jawab secara perdata baik perbuatan melawan hukum maupun tanggung jawab terhadap konsumen, tanggung jawab administratif yang dilakukan oleh badan yang berwenang, serta tanggung jawab pidana berdasarkan hukum positif yang ada.

Bab terakhir adalah BAB IV yang berisikan kesimpulan dan saran yang menjawab pokok permasalahan dalam penulisan ini.

BAB II

Tanda Tangan Elektronik dan Transaksi Elektronik

2.1. Komunikasi Elektronik dan Transaksi Elektronik

2.1.1. Komunikasi Elektronik

Dalam arti sempit, komunikasi merupakan suatu proses penyampaian informasi melalui media tertentu. Dalam arti luas, *United Nations Convention on the Use of Electronic Communications in International Contracts* pada tahun 2005 (selanjutnya akan disebut dengan *Electronic Communication Convention* atau disingkat dengan ECC) mendefinisikan komunikasi sebagai berikut: *"communication means any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract."* Komunikasi juga dapat dikatakan sebagai suatu interaksi, kontak, hubungan penyampaian dan penerimaan pesan (informasi) antar pihak agar pesan tersebut dapat dipahami dan ditafsirkan serta timbulnya pengertian bersama. Berdasarkan pengertian ini, komunikasi adalah suatu interaksi antar 2 (dua) pihak atau lebih yang merupakan proses penyampaian informasi atau pesan berupa pernyataan, permintaan, pemberitahuan, termasuk tawaran dan penerimaan penawaran dimana para pihak ditujukan dapat memahami, menafsirkan serta timbul pengertian yang sama melalui media (medium) tertentu.

Sedangkan komunikasi elektronik didefinisikan pada ECC sebagai berikut: *"Electronic communication means any communication that the parties make by means of data messages"*. Komunikasi elektronik merupakan komunikasi yang dibuat oleh para pihak melalui pengolahan data. *Data message* merupakan informasi yang dihasilkan, dikirimkan, diterima atau disimpan dengan cara elektronik, magnetik, optik atau yang serupa, tidak terbatas pada pertukaran data elektronik,

surat elektronik, telegram dan sebagainya.[31] Informasi yang disampaikan ini dapat berupa audio, video atau berupa teks. Dalam proses pengiriman informasi dibutuhkan suatu mekanisme yang menghubungkan antara pengirim informasi (*source*) dengan penerima informasi (*destination*). Mekanisme tersebut sering juga disebut sistem informasi. Sistem informasi merupakan sistem untuk menghasilkan, pengiriman, penerimaan, penyimpanan atau pengolahan data.[32]

2.1.2. Transaksi Elektronik

Menurut Richter dan Furubotn, transaksi merupakan perpindahan barang, jasa, informasi, pengetahuan dan lain-lain dari satu tempat (komunitas) ke tempat (komunitas) lain atau pemindahan barang dari produsen ke konsumen atau pemindahan barang dari satu individu ke individu yang lain.[33] Hal ini disebut dengan transaksi fisik. Selain dalam pengertian perpindahan fisik, transaksi juga meliputi pemindahan hak kepemilikan atas barang dari pemilik ke pihak lain dimana hal ini disebut transaksi dari aspek legal.[34] Max Weber menyatakan transaksi merupakan tindakan yang diperlukan untuk menetapkan, memelihara dan atau mengubah hubungan sosial.[35] Definisi transaksi secara tidak langsung dijabarkan di dalam hukum nasional pula sebagai bentuk dari suatu perjanjian, dalam hal ini pasal 1320 KUHPerdata. Pasal 1320 KUHPerdata menentukan empat syarat sahnya perjanjian yaitu harus ada:

1. Kesepakatan kedua belah pihak,
2. Kecakapan untuk melakukan perbuatan hukum,

---

[31] Definisi *data message* pada *United Nations Convention on the Use of Electronic Communications in International Contracts*: *"Data message means information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy."*

[32] Definisi sistem informasi berdasarkan *United Nations Convention on the Use of Electronic Communications in International Contracts: "Information system means a system for generating, sending, receiving, storing or otherwise processing data messages."*

[33] Aceng Hidayat, Modul Mata Kuliah Pengantar Ekonomi Kelembagaan, 2007, Institut Pertanian Bogor, 2007, diunduh pada http://www.scribd.com/doc/47760007/9/Definisi-Transaksi.

[34] *Ibid.*

[35] *Ibid.*

3. Obyek (Sesuatu yang diperjanjikan dalam suatu perjanjian haruslah suatu hal atau barang yang cukup jelas), dan
4. Kausa yang halal.

Syarat pertama dan ke dua disebut syarat subyektif. Apabila syarat subyektif tidak terpenuhi, maka perjanjian dapat dimintakan pembatalan lewat pengadilan. Jika tidak dituntut pembatalan, maka perjanjian tetap berlaku. Sedangkan syarat ke tiga dan keempat disebut syarat obyektif yang mana jika syarat obyektif ini tidak dipenuhi, maka perjanjian batal demi hukum atau dianggap tidak pernah ada. Berdasarkan definisi di atas, transaksi merupakan pertemuan kesepakatan dalam menetapkan, memelihara dan atau mengubah hubungan sosial baik menyangkut perpindahan barang ataupun jasa.

Transaksi dalam bidang teknologi saat ini semakin berkembang. Adapun transaksi dalam bidang ini disebut juga dengan transaksi elektronik. Transaksi elektronik merupakan salah satu bentuk transaksi yang bersifat *non-face* dan *non-sign* (tanpa bertatap muka dan tanpa tanda tangan). Transaksi ini bersifat *paperless* (tanpa dokumen tertulis), *borderless* (tanpa batas geografis) dan para pihak yang melakukan transaksi tidak perlu bertatap muka. Hal tersebut dipertegas dengan adanya UNCITRAL (United Nations Commission on International Trade Law, Model Law on Electronic Commerce, 1998) yang mendefinisikan *e-commerce* (*electronic commerce*) sebagai: *Electronic commerce, which involves the use of alternatives to paper-based methods of communication and storage of information.*[36] Transaksi dalam hal ini dinyatakan sebagai suatu metode komunikasi dan penyimpanan informasi yang menggunakan alternatif media (medium) di luar hal yang tertulis di dalam kertas (informasi atau dokumen yang ditulis di atas kertas).

Sedangkan menurut Peter Scisco, *e-commerce* lebih diartikan sebagai pertukaran barang dan jasa melalui internet dan lebih mengacu pada transaksi jual beli saja. Adapun definisi yang diberikan sebagai

[36] UNCITRAL, *Model Law on Electronic Commerce*, 1998, diunduh pada www.uncitral.org.

berikut: *Electronic Commerce or e-commerce, the exchange of goods and services by means of the internet or other computer networks. E-commerce follows the same basic principles as traditional commerce – that is, buyers and sellers come together to exchange goods for money. But rather than conducting business in the traditional way – in stores and other "brick and mortar" buildings or through mail order catalogs and telephone operators – in e-commerce buyers and sellers transact business over networked computers.*[37]

Transaksi Elektronik juga didefinisikan di dalam Pasal 1 ayat (9) UU ITE yang berbunyi: "Transaksi elektronik adalah hubungan hukum yang dilakukan melalui komputer, atau media elektronik lainnya." Berdasarkan definisi ini, transaksi elektronik memunculkan akibat hukum terhadap subyek hukum yang telah melakukan transaksi tersebut. Melihat pengertian di atas, transaksi elektronik (*e-commerce*) merupakan transaksi perdagangan yang mengakibatkan hubungan hukum antara para pihak yang melakukan pertukaran informasi atau data (barang dan jasa) yang memiliki prinsip dasar sama dengan transaksi konvensional, namun dilakukan melalui media elektronik dalam hal ini media yang tidak berwujud (internet) di mana para pihak tidak perlu bertatap muka secara fisik. Berdasarkan berbagai definisi yang telah dipaparkan, dapat ditarik beberapa unsur dalam transaksi elektronik, yaitu:

1. Mengakibatkan timbulnya hubungan hukum atau perbuatan hukum antara subyek hukum (antara dua pihak atau lebih),
2. Ada pertukaran barang dan jasa,
3. Menggunakan internet sebagai media utama dalam melakukan transaksi, dan
4. Memiliki prinsip dasar yang sama dengan transaksi konvensional (transaksi yang ditulis di atas kertas).

[37] Peter Scisco, *Electronic Commerce*, dalam Microsoft Encarta Online, Encyclopedia 2006, Microsoft Corporation 1997-2006, http://encarta.msn.com.

Perbuatan hukum yang timbul dalam transaksi elektronik ini dapat dilaksanakan melalui 2 (dua) konteks, yaitu:[38]

1. Hubungan penyelenggara negara kepada publiknya (pelayanan publik), dan
2. Hubungan perdata para pihak untuk melakukan perikatan atau kontrak elektronik.

Baik dalam pelayanan publik maupun privat, suatu komunikasi elektronik bersifat privat hanya antara para pihak saja (baik B2B, B2C, C2C, G2C).[39] Selanjutnya jenis-jenis *e-commerce* tersebut akan diuraikan di bawah ini:[40]

a) <u>*Bussiness to Bussiness*</u>

Transaksi *bussines to bussiness* atau yang sering disebut *b to b* adalah transaksi antar perusahaan (baik pembeli maupun penjual adalah perusahaan). Biasanya antara mereka telah saling mengetahui satu sama lain dan sudah terjalin hubungan yang cukup lama. Pertukaran informasi hanya berlangsung diantara mereka dan pertukaran informasi itu didasarkan pada kebutuhan dan kepercayaan. Perkembangan *b to b* lebih pesat jika dibandingkan dengan perkembangan jenis *e-commerce* yang lainnya.

b) <u>*Bussiness to Customer*</u>

Bussiness to customer atau yang dikenal dengan *b to c* adalah transaksi antara perusahaan dengan konsumen/individu. Contohnya adalah *amazon.com* sebuah situs *e-commerce* yang besar dan terkenal. Pada jenis ini, transaksi disebarkan secara umum, dan konsumen yang berinisiatif melakukan transaksi. Produsen harus siap menerima respon dari konsumen tersebut. Biasanya sistem yang digunakan adalah *website* karena sistem ini yang sudah umum dipakai di kalangan masyarakat.

[38] Edmon Makarim, *Tanggung Jawab Penyelenggara Sistem Elektronik, Op.Cit.*, hlm.40.
[39] *Ibid.*
[40] Edmon Makarim, *Hukum Telematika*, PT RajaGrafindo Persada, Jakarta, 2005, Hlm. 227.

c) *Customer to Customer*

Customer to customer ini adalah transaksi dimana individu saling menjaul barang pada satu sama lain. Contohnya adalah individu menjual sesuatu yang diklasifikasikan antara lain kepemilikan kediaman *(residential property)*, mobil dan lain-lain. Pengiklanan jasa personal di internet dan menjual ilmu pengetahuan dan keahlian merupakan contoh lain dari C to C beberapa situs pelelangan *(action)* membolehkan individu untuk meletakkan barang. Pada akhirnya banyak individu menggunakan internet dan jaringan organisasi internal lainnya ke pelelangan barang untuk penjual atau pelayanan.

d) *Customer to Business*

Customer to bussines yaitu transaksi yang memungkinkan individu menjual barang pada perusahaan.

e) *Customer to Government*

Customer to government adalah transaksi dimana individu dapat melakukan transaksi dengan pihak pemerintah, seperti membayar pajak.

Pembagian jenis transaksi komersial elektronik (*e-commerce*) tersebut di atas hampir sama dengan pembagian menurut Efraim Turban yang membagi transaksi komersial elektronik (*e-commerce*) menjadi:

1. *Business to Business* (B2B),
2. *Business to Consumer* (B2C),
3. *Consumer to Consumer* (C2C),
4. *Consumer to Business* (C2B),
5. *Nonbusiness e-commerce*,
6. *Intrabusiness organizational e-commerce*[41]

[41] Hasanuddin Rahman, *Seri Keterampilan Merancang Kontrak Bisnis, Contract Drafting*, Bandung, PT. Citra Aditya Bakti, 2003.

Berdasarkan konsekwensinya terhadap komunikasi tersebut dipersyaratkan adanya jaminan suatu komunikasi yang aman (*secured communication*) yang mensyaratkan adanya:

1. Keontentikan suatu pesan (*authenticity*),
2. Otorisasi kewenangan atau kapasitas hukum pihak yang melakukan (*authorization*),
3. Kerahasiaan pesan yang dikomunikasikan (*confidentiality*),
4. Keutuhan pesan yang dikomunikasikan (*integrity*),
5. Ketersediaannya (*availability*), dan
6. Tidak dapat disangkal (*non-repudiation*).[42]

Di dalam transaksi elektronik, proses terciptanya penawaran dan penerimaan tersebut menimbulkan suatu kesepakatan, dimana kesepakatan tergantung kepada prosedur-prosedur dalam sistem penawaran diterima (saat *offer* di-*accept*). Pada *United Nations Convention on the Use of Electronic Communications in International Contracts* artikel 11 mengenai *invitations to make offers* dinyatakan bahwa: *"A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including proposals that make use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance."* Berdasarkan hal ini, segala jenis penawaran tidak diartikan sebagai kesepakatan apabila tidak adanya sisi kesepakatan dalam penawaran tersebut. Penawaran di dalam pengertian ini hanya sebatas penawaran kepada siapa saja yang mengakses program atau situs tertentu yang menawarkan sesuatu hal, namun pada hakekatnya belum tercapainya suatu kesepakatan karena belum adanya permintaan yang menyatakan sepakat terhadap penawaran tersebut.

[42] Edmon Makarim, *Tanggung Jawab Penyelenggara Sistem Elektronik, Op.Cit.*, hlm.40.

The United Nations Conference on International Trade Law (UNCITRAL) telah menetapkan suatu *model law* untuk *electronic commerce*[43] pada tahun 1996 yang kemudian direvisi pada tahun 1998. Model hukum tersebut berisi panduan-panduan yang disarankan diikuti oleh negara-negara anggota saat mereka membuat legislasi untuk *e-commerce* (atau transaksi elektronik secara umum). Adapun yang termaktub dalam *model law* tersebut antara lain adalah masalah:[44]

a) Keberadaan dan pengakuan hukum transaksi elektronik
b) Pengakuan konsep *incorperation by reference*
c) Jaminan keamanan atas keaslian transaksi elektronik dengan tanda tangan elektronik ataupun dengan cara lainnya yang dapat dipercaya dan diandalkan
d) Penggunaan salinan transaksi elektronik
e) Pengarsipan transaksi elektronik
f) Otomasi transaksi elektronik
g) Hak dan kewajiban pengiriman transaksi elektronik dan penerima transaksi elektronik
h) Tanda penerimaan tanda bukti (*acknowledgement of receipt)* sebagai tanda untuk mengeksekusi transaksi
i) Kapan dikirim, diterima, terjadi dan berlaku transaksi elektronik

Mengenai pengaturan kontrak elektronik, maka dapat dilihat pada ketentuan *model law on Electronic Commerce*, pasal 15 *Model Law on Elektronic Commerce* menyatakan:[45]

1. Kecuali diatur secara lain oleh originator dan *addresse*, saat suatu *data massage* dikirim (*dispatch)* adalah pada saat ia memasuki suatu

[43] Patut dicatat sebenarnya model law ini sebelumnya dinamakan model law for EDI (*Electronic Data Interchange),* namun pada saat terakhir diganti namanya menjadi *model law for e-commerce,* meskipun demikian, prinsip-prinsip yang ada didalamnya juga dapat diterapkan untuk transaksi perdagangan elektronik secara umum. Karena *model law* untuk *e-commerce* UNCITRAL telah memuat prinsip-prinsip umum yang cukup universal untuk berbagai jenis transaksi elektronik.

[44] Diunduh pada http://www.indocybeerlawnet.

[45] Budi Agus Riswandi, *Aspek Perlindungan Nasabah dalam Sistem Pembayaran Internet,* Jurnal Hukum Lus Wuila Iustu, Fakultas Hukum Universitas Islam Indonesia, 2002, Hlm. 82.

sistem informasi di luar kontrol dari originator atau orang lain yang mengirimkan data tersebut untuk kepentingan originator.

2. Kecuali diatur secara lain antara *originator* dan *addresse,* waktu diterimanya suatu data *massages* ditentukan sebagai berikut: kalau seorang *addresse* sudah menentukan suatu informasi sebagai tujuan dikirimnya *data massage,* saat diterimanya adalah:
   a) Pada saat *data massage* tersebut memasuki sistem informasi tertentu (*designated system information)* yang dituju, atau
   b) Apabila suatu *data message* dikirimkan ke suatu informasi yang bukanlah suatu sistem informasi tertentu (*designated system information),* maka waktunya adalah pada pesan tersebut diterima oleh *addresse.*

Untuk masalah jaminan keamanan di dalam transaksi *e-commerce* dikenal ada dua metode yang dipakai kebanyakan pedagang *online* yaitu:[46]

a. Metode atau instrumen *Secure Sockets Layer* (SSL)

   Secure Sockets Layers (SSL) adalah instrumen yang sudah dipakai. SSL melindungi informasi pribadi dalam kontrak antara konsumen dengan pedagang. Keamanan data yang dikirim melalui jaringan juga terjamin. Konsumen dalam melakukan transaksi harus memastikan bahwa data-data tersebut sudah dalam bentuk terenkripsi dengan baik. Hal tersebut dapat diperiksa dan dipastikan melalui tampilan sebuah icon kecil dalam bentuk gambar sebuah kunci saat melakukan *browsing,* gambar kunci tersebut tidak boleh rusak atau patah. Selain melihat gambar kunci tersebut, dapat juga diperiksa situs penjual yang biasanya diawali dengan http harus menjadi https pada saat proses transaksi.

b. Metode yang kedua adalah *Secure Electronic Transaction* (SET)

   SET menggunakan sertifikasi digital untuk membuktikan bahwa konsumen dan pedagang memiliki hak untuk menggunakan dan

[46] Edmon Makarim, *Op. Cit.*, Hlm.231.

menerima kartu. Visa telah menggunakan metode ini. SET adalah alat elektronik yang berfungsi untuk memverifikasi pedagang di layar dan juga berfungsi bagi penjual/*merchant* untuk memeriksa tanda tangan konsumen pada bagian belakang kartu visa. SET memberikan cara bagi pemegang kartu dan pedagang untuk mengidentifikasi satu sama lain sebelum melakukan transaksi sehingga pembayaran dapat terjamin kebenarannya.

2.2. Tanda Tangan Elektronik (TTE) dan Sertifikasi Elektronik

2.2.1. Tanda Tangan Pada Umumnya

Pengertian tanda tangan dalam arti umum, adalah tanda tangan yang dapat didefinisikan sebagai suatu susunan (huruf) tanda berupa tulisan dari yang menandatangani, dengan mana orang yang membuat pernyataan atau keterangan tersebut dapat di individualisasikan.[47] Definisi ini menyatakan bahwa setiap pernyataan atau keterangan yang dibuat secara tertulis harus dibubuhi tanda tangan dari yang bersangkutan.

Menurut Kamus Besar Bahasa Indonesia, pengertian tanda tangan adalah tanda sebagai lambang nama yang dituliskan dengan tangan oleh orang itu sendiri sebagai penanda (telah menerima). Pengertian disini menyatakan bahwa tanda tangan merupakan suatu penandaan yang menunjukkan kepada orang yang menandatangani. Menurut *American Bar Association* (ABA), pengertian tanda tangan dapat berupa tanda apapun yang dibuat dengan tujuan untuk memberikan persetujuan dan otentifikasi terhadap suatu dokumen tersebut.[48] Pengertian ini tentunya

[47] Herlien Budiono, Kumpulan Tulisan Hukum Perdata Di Bidang Kenotariatan, PT.Citra Aditya Bakti, Bandung, 2007, Hlm. 220.

[48] Information Security Committee, Section of Science & Technology – American Bar Association, Digital Signature Guideliness (United States, American Bar Association: 1996), hlm. 4. Pengertian dari otentifikasi menurut ABA adalah "*authentication is generally the process used to confirm the identity of a person or to prove the integrity of specific information. More specifically, in the case of a message, authentication involves determining its source and providing assurance that the message has not been modified or replaced in transit. The historical legal concept of signature is broader. It recognizes any mark made with the intention of authenticating the marked document*".

lebih luas ketimbang dua definisi sebelumnya, dalam ABA, tanda tangan selain menyatakan persetujuan juga menyatakan otentifikasi terhadap dokumen yang ditanda tangani.

Hukum positif Indonesia belum pernah memberikan definisi terhadap tanda tangan yang sesungguhnya mempunyai dua fungsi hukum dasar, yaitu: (1) tanda identitas Penandatanganan, dan (2) sebagai tanda persetujuan dari Penandatanganan terhadap kewajiban-kewajiban yang melekat pada akta.[49] Berdasarkan kedua fungsi hukum ini maka dapat ditarik suatu definisi bahwa tanda tangan adalah sebuah identitas yang berfungsi sebagai tanda persetujuan terhadap kewajiban-kewajiban yang melekat pada akta.[50] Definisi ini menyatakan bahwa adanya kewajiban yang muncul atas akibat dari tanda tangan tersebut.

Keberadaan suatu tanda tangan adalah merepresentasikan adanya suatu tindakan verifikasi dari si penandatangan terhadap apa yang ditandatanganinya, karenanya penandatangan selayaknya membaca terlebih dahulu dan memeriksa informasi tersebut kemudian membubuhkan identitas dirinya sebagai subyek hukum yang bertanggung jawab atas informasi tersebut.[51] Tindakan penandatangan tersebut juga memperlihatkan suatu niatan (*intention*) atau persetujuan dari si penandatangan terhadap sesuatu, baik substansi informasi yang terkandung didalamnya sesuai dengan tujuan dari penggunaan tandatangannya.[52] Penandatangan sebagai subyek hukum memiliki kewajiban terhadap segala hal yang telah ditanda tanganinya sesuai dengan apa yang menjadi manfaat dari hal yang ditandatangani.

The notions of "authentication" and "authenticity" are generally understood in law to refer to the genuineness of a document or record, that is, that the document is the "original" support of the information it contains, in the form it was recorded and without any alteration. Signatures, in turn, perform three main functions in the paperbased

[49] Fairuz El Said, Cyber Law-Tanda Tangan Digital, 15 Agustus 2010.
[50] *Ibid.*
[51] Edmon Makarim, *Notaris dan Tanda Tangan Elektronik.* Cetakan Pertama. Jakarta: PT. Rajawali Grafindo Persada. 2011. Hlm.41.
[52] *Ibid.*

environment: signatures make it possible to identify the signatory (identification function); signatures provide certainty as to the personal involvement of that person in the act of signing (evidentiary function); and signatures associate the signatory with the content of a document (attribution function). Signatures can be said to perform various other functions as well, depending on the nature of the document that was signed. For example, a signature might attest to the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text (thus displaying awareness of the fact that legal consequences might possibly fl ow from the act of signing); the intent of a person to associate him or herself with the content of a document written by someone else; and the fact that, and the time when, a person has been at a given place.[53]

Berdasarkan pengertian di atas, tanda tangan memiliki tiga fungsi utama, yaitu:

1. Identifikasi: untuk mengidentifikasi penandatangan,
2. Pembuktian: untuk memberikan kepastian mengenai keterlibatan pribadi orang tersebut di dalam penandatanganan (fungsi pembuktian), dan
3. Atribusi: untuk mengasosiasikan penandatangan dengan isi dokumen.

Penandatanganan sebuah dokumen secara umum mempunyai tujuan atau fungsi sebagai berikut:[54]

1. Bukti (*evidence)*

   Suatu tandatangan akan mengotentifikasikan penandatangan dengan dokumen yang ditandatanganinya. Pada saat penandatanganan membubuhkan tanda tangan dalam suatu bentuk yang khusus, tulisan tersebut akan mempunyai hubungan (*attribute)* dengan penandatangan.

[53] *UNCITRAL Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods.* Hlm. 5 Angka (7).

[54] Vollmar, *Pengantar Studi Hukum Perdata*, Jilid II (Jakarta: Raja Grafindo Persada, 1998), hlm. 142.

2. *Ceremony*

   Penandatanganan suatu dokumen akan berakibat penandatangan akan tahu bahwa ia telah melakukan suatu perbuatan hukum, sehingga akan mengeliminasi kemungkinan adanya *inconsiderate engagement*. Penandatanganan suatu dokumen 'memaksa' pihak yang menandatangani untuk mengakui pentingnya dokumen tersebut.

3. Persetujuan *(approval)*

   Dalam penggunaannya dalam berbagai konteks baik oleh hukum atau oleh kebiasaan, tanda tangan melambangkan adanya persetujuan atau otorisasi terhadap suatu tulisan, atau penandatangan telah secara sadar mengetahui bahwa tanda tangan tersebut mempunyai konsekuensi hukum.

4. *Efficiency and Logistics*

   Tanda tangan dalam suatu dokumen tertulis seringkali menimbulkan kejelasan dan keabsahan dari suatu transaksi dan juga akan mengurangi kebutuhan untuk mengecek keabsahan suatu dokumen kepada orang yang bersangkutan, sedangkan dalam pasal 187 KUHP (kitab undang-undang hukum acara pidana, undang-undang nomor 8 tahun 1981), disebutkan bahwa pengadilan juga menerima segala macam tulisan/surat, baik tulisan/surat yang bertandatangan maupun yang tidak ditandatangani.

Dalam pengertian ini ditambah satu aspek yaitu adanya keabsahan dalam suatu dokumen ataupun transaksi yang ditanda tangani. Dalam mencapai tujuan atau fungsi dari penandatanganan suatu dokumen seperti yang telah disebutkan di atas, sebuah tanda tangan harus mempunyai atribut-atribut sebagai berikut:

a. Otentikasi Penandatangan: sebuah tanda tangan seharusnya dapat mengidentifikasikan siapa yang menandatangani dokumen tersebut sehingga sulit untuk ditiru orang lain.

b. Otentikasi Dokumen: sebuah tanda tangan seharusnya mengidentifikasi apa yang ditandatangani, membuatnya tidak mungkin dipalsukan ataupun diubah (baik dokumen yang ditandatangani maupun tandatangannya) tanpa diketahui.[55]

Otentikasi penandatangan dan dokumen adalah alat untuk menghindari pemalsuan dan merupakan suatu penerapan konsep *nonrepudiation* dalam bidang keamanan informasi (dalam hal ini termasuk dalam salah satu aspek *secured communication*). *Nonrepudiation* adalah jaminan dari keaslian ataupun penyampaian dokumen asal untuk menghindari penyangkalan dari penandatangan dokumen (bahwa dia tidak menandatangani dokumen tersebut) serta penyangkalan dari pengirim dokumen (bahwa dia tidak mengirimkan dokumen tersebut).[56] Kebutuhan dari segi keamanan dari suatu transaksi legal sangat diperlukan mengingat mudahnya pemalsuan akan dokumen sehingga konsep ini mempunyai peran penting dalam menjamin suatu transaksi legal yang bersangkutan benar adanya dan sesuai dengan aslinya.

2.2.2. Tanda Tangan Elektronik (TTE)

Tanda tangan secara konvensional dikenal dengan susunan tanda yang dibubuhi di dalam suatu dokumen atau di atas kertas sebagai tanda orang yang menandatanganinya. Seiring dengan kebutuhan yang semakin kompleks dan teknologi yang semakin modern yang dapat melakukan berbagai aktivitas dengan instan, maka semakin diperlukannya jaminan akan keamanan dalam aktivitas tersebut. Perkembangan inilah yang melahirkan TTE yang berarti merepresentasikan adanya suatu keotentikan dan keaslian suatu tanda tangan, dokumen ataupun informasi elektronik baik berimplikasi pada hukum ataupun tidak sehingga menambah keamanan di dalam aktivitas yang bersangkutan.

[55] *Ibid.*
[56] *Ibid.*

Pengertian TTE tertuang pada Pasal 1 ayat (12) Undang-Undang Nomor 11 Tahun 2008 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 autentifikasi". Berdasarkan definisi dalam pasal ini menyatakan bahwa penandatangan merupakan subyek hukum yang terasosiasi atau terkait dengan tanda tangan elektronik yang digunakan sebagai alat verifikasi dan autentifikasi.

Electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.[57] Berdasarkan definisi ini, TTE diartikan sebagai data elektronik yang terkait atau terhubung dengan data elektronik lainnya, yang berfungsi sebagai alat otentikasi. TTE 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.[58] Sedangkan dalam pengertian ini, TTE merupakan data yang berisi kode pesan digital hanya untuk memberikan jaminan atas keaslian data tersebut.

Merujuk pada UNCITRAL, ASEAN juga telah membahas permasalahan mengenai TTE sejak 2001 dengan adanya E-ASEAN *Reference Framework for Electronic Commerce Legal Infrastructure*, yang menjelaskan bahwa: *a digital signature, on the other hand, is an "electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine (a) whether the transformation was created using the private key that corresponds to the*

[57] *Directive 1999/93/EC of The European Parliament and of The Council.* 13 Desember 1999. *On a Community framework for electronic signatures*. *Article* 2 no 1.

[58] Soemarno Partodiharjo, *Tanya Jawab Sekitar Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*, PT. Gramedia Pustaka Utama, Jakarta, 2009, Hlm.21.

signer's public key; and (b) whether the initial electronic record has been altered since the transformation was made". A digital signature is thus more secure and tamper-proof than an electronic signature.[59] Berdasarkan hal ini, ada beberapa negara yang mengatur ketentuan mengenai TTE, seperti:

a. *Electronic Transactions Act (ETA) of Singapore*

b. *Digital Signature Act (DSA) of Malaysia*

c. *Electronic Commerce Act (ECA) of Philippines*

d. *Electronic Transactions Order (ETO) of Brunei*

e. *Draft Electronic Transactions Bill (ETB) of Thailand*

f. *Electronic Commerce (AEC) of Vietnam*

Terdapat pula beberapa pengaturan baik secara internasional (UNCITRAL dan ECC), regional (*European Community Directive*) maupun nasional (seperti UETA di Amerika Serikat, UU ITE di Indonesia dan lain sebagainya. Beberapa karakteristik perbedaan tersebut dapat diliat di dalam tabel berikut ini:

UNCITRAL Model Law E-signatures (2001)	**EC Directive: 1999/93/EC**	**US: E-sign & UETA**
• Art.1 Sphere of Application • Art.2 Definitions • Art.3 Equal treatment of signature tech • Art.4 Interpretation • Art.5 Variation by agreement • Art.6 Compliance with a requirement of a signature • Art.7 Satisfaction of Article 6 • Art.8 Conduct of the signatory • Art.9 Conduct of Certification Service Provider • Art.10 Trustworthiness • Art.11 Conduct of Relying Party • Art.12 Recognition of Foreign Certificates and Electronic Signatures.	• Art.1 Scope • Art.2 Definitions • Art.3 Market Access • Art.4 Internal Market Principles • Art.5 Legal Effects of E-signatures • Art.6 Liability • Art.7 International Aspect • Art.8 Data Protection • Art.9 Committe • Art.10 Tasks of the Committe • Art.11 Notification • Art.12 Review • Art.13 Implementation • Art.14 Entry into Force • Art.15 Addresses • Annex-1 Requirement for Qualified Certificates • Annex-2 Requirement for	Sect.1. Short Title Sect.2. Definitions Sect.3. Scope Sect.4. Prospective Application Sect.5. Use of Electronic Records and Electronic Signatures; Variation by Aggrement Sect.6. Construction adn Application Sect.7. Legal Recognition of Electronic Signatures, and Electronic Contracts Sect.8. Provision of Information in Writing; Presentation of Records Sect.9. Attribution and Effect of Electronic Record and Electronic Signature Sect.10. Effect of Change or Error Sect.11. Notarization and Acknowledgment

[59] E-ASEAN *Reference Framework for Electronic Commerce Legal Infrastructure* E-ASEAN 2001, hlm. 3.

	Certification Service Providers Issuing Qualified Certificates • Annex-3 Requirement for Secure Signature Creation Devices • Annex-4 Recommendation for Secure Signature Verification	Sect.12. Retention of Electronic Records; Originals Sect.13. Admissibility in Evidence Sect.14. Automated Transaction Sect.15. Time and Place of Sending and Receipt Sect.16 Transferable Records Sect.17. Creation and Retention of Electronic Records and Conversion of Written Records by Governmental Agencies Sect.19. Interoperability Sect.20. Severability Clause Sect.21. Effective Date

Tabel 1: Perbandingan Struktur Ketentuan E-signatures antara UNCITRAL, EC Directive dan UETA[60]

United Nation Commission on International Trade Law (UNCITRAL) sebelumnya telah menetapkan *Model Law on E-Commerce* (1996) dan *Model Law on E-Signature* (2001), kemudian dalam perkembangannya melahirkan *United Convention on the Use of E-Communication in International Contracts* (2005) yang mencakup tentang *e-commerce* dalam lingkup antar pelaku usaha (B2B). Selanjutnya menetapkan pengaturan akan keabsahan tanda tangan elektronik dalam *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods* (2009) merupakan langkah besar dalam verifikasi dan autentifikasi sehingga menciptakan rasa aman dalam bertransaksi.

Dalam menciptakan rasa aman, sebagaimana lazimnya dipahami terhadap keberadaan suatu tanda tangan secara konvensional, maka paling tidak ada beberapa fungsi dari TTE itu sendiri, yakni:

(i) Fungsi simbolik dari otorisasi seseorang dimana dengan pembubuhan identitas suatu subyek hukum yang bertanggung-jawab, bahwa apa yang dituliskan atau disampaikan, selain merepresentasikan karakteristik identitas dari seseorang (meskipun terdapat kesamaan nama orang, namun ekspresi

[60] Edmon Makarim, *Notaris dan Tanda Tangan Elektronik, Op.Cit.,* Hlm.46.

tanda tangannya akan selalu berbeda) dan juga kewenangannya;

(ii) Fungsi otentikasi bahwa apa yang ditandatanganinya telah dibacanya dan diketahuinya serta dikunci dengan keberadaan pencantuman namanya (contoh: dalam pembuatan suatu perjanjian maka terdapat paraf setiap halaman yang telah dibacanya);

(iii) Fungsi persetujuan bahwa tindakan penandatanganan adalah penjelmaan dari suatu tindakan persetujuan atau penerimaan terhadap konten didalamnya;

(iv) Fungsi pembuktian bahwa selanjutnya bahwa konten atas informasi tersebut akan menjadi bukti hukum bagi para pihak yang menggunakannya.[61]

Tidak jauh berbeda dengan konvensional, pada dasarnya suatu tanda tangan elektronik adalah berfungsi yang sama sebagaimana layaknya suatu tandatangan di atas kertas. Hal ini disebut dengan istilah "*functional equivalent approach*" yakni suatu pendekatan yang mempersamakan suatu tandatangan elektronik secara fungsional dengan suatu tandatangan elektronik di atas kertas.[62]

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:[63]

a. *Autenthicity*

Dengan memberikan *digital signature* pada data elektronik yang dikirimkan, maka akan dapat atau bisa ditunjukkan dari mana data-data elektronik tersebut sesungguhnya berasal. Terjaminnya

[61] Edmon Makarim, *Op.Cit.*, Hlm.43.
[62] *Ibid.*, Hlm.43-44.
[63] Arianto Mukti Wibowo, *kerangka Hukum Digital Signature Dalam Electronic Commerce*, 1999, amwibowo@caplin.cs.ui.ac.id, Hlm. 3.

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:

1. Identitas
2. Kewenangan
3. Kedudukan hukum
4. 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 kualifikasi ini adalah apabila suatu perusahaan 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 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 atau 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 bebeda 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.

Sedangkan menurut Schellekens dalam bukunya yang berjudul *Electronic Signatures*, tanda tangan elektronik memiliki fungsi sebagai berikut:[64]

1. Authentication
   Authentication is the act of the authenticator by which he earmarks a document as being authentic and in doing so confirms its authenticity. The authenticity concerns several aspects of the signed document:
   a. Authenticity with respect to the person of the authenticator,
   b. Authenticity with respect to the declaration,
   c. Authenticity with respect to the contents of the declaration.

[64] M.H.M. Schellekens, *Electronic Signatures*, Belanda: Cambridge University Press, 2004. Hlm. 59-71.

2. Identification
   On this basis, an identity is that which ensures that one is who one claims to be. A means of identification ideally has the following properties:
   a. It has to be unique. Different persons have different signatures,
   b. It points to the person that is to be identified.
   c. The person identified by the means of identification is the only person that can create the means of identification, or his or her co-operation is necessary.
3. Authorisation
   Authorisation has more than one meaning:
   a. By signing a document containing a declaration, the signatory declares implicity that he is authorised to make the declaration and to perform the associated legal act.
   b. Also be used to indicate a successful verification of somebody's authority to do something.
   c. May be used within the meaning of giving authority. Example, i may authorise somebody to act on my behalf, in my name; authorisation then has the meaning of granting power to attorney.
4. Integrity
   Integrity indicates that data in a document have not been altered, deleted or supplemented, irrespective of whether this has come about through natural causes or through manipulation.
5. Originality
   Originality refers to the characteristic that a document is an original, i.e., that it is not a copy.

2.2.3. Jenis TTE dan bobot pembuktiannya

Sesuai perkembangan teknologi, terdapat beberapa moda tentang suatu tanda tangan elektronik, yakni:

(i) penggunaan kata kunci (*password*) ataupun kombinasinya (*hybrid methods*), dan

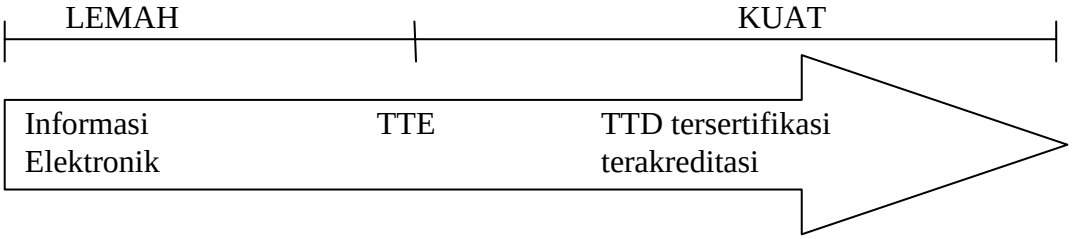
(ii) tanda tangan digital yang dipindai secara (*scanned signatures*) atau pengetikan nama pada suatu informasi (*typed names*),

(iii) penggunaan fitur tombol tanda persetujuan atau tanda penerimaan secara elektronik (*OK button* atau *Accept button*) yang ditunjang dengan saluran komunikasi yang aman (*Secure Socket Layer*),

(iv) penggunaan tanda yang unik pada anggota badan (*biometric*),

(v) pengunaan tanda tangan digital yang berbasiskan enkripsi suatu pesan (*digital signatures).*[65]

Semua jenis tanda tangan elektronik, sesuai karakteristiknya secara teknis akan mempunyai level kekuatan pembuktian yang berbeda sesuai kaedah-kaedah yang berlaku dalam *secured communication*.[66] Semakin jelas sistem keotentikannya yang berdampak kepada kepastian nir-sangkal maka akan semakin kuat pula tingkat atau bobot pembuktiannya. Sementara itu, dalam prakteknya keberadaan suatu metode jika tidak melibatkan pihak ketiga tentunya akan tetap menyimpan potensi adanya penampikan dari seseorang.[67] Oleh karena itu, hal tersebut perlu ditunjang dengan keberadaan suatu sertifikasi elektronik yang diselenggarakan oleh pihak ketiga (*Certification Service Provider*) sebagai pihak pengemban amanat kepercayaan tersebut (*Trusted Third Party*).[68]



	Confidentiality	Integrity	Authenticity	Authorization	Non-Repudiation
Lemah	x	x	x	x	x
Intermediate	v	v	v	v	x
Kuat	v	v	v	v	v

Gambar 1. Tingkatan Nilai Kekuatan Pembuktian Informasi Elektronik[69]

[65] Edmon Makarim, *Notaris dan Tanda Tangan Elektronik, Op.Cit.,* Hlm.44.

[66] Semakin memenuhi *Secured Communication* yang meliputi *Confidentiality, Integrity, Authorization, Availability, Authenticity, Non-Repudiation, dan Auditability/* CIAANA, maka semakin kuat level pembuktiannya.

[67] Edmon Makarim, *Op.Cit.,* Hlm.44-45.

[68] *Ibid.*

[69] Menyesuaikan dengan gambar pada buku Edmon Makarim yang berjudul Notaris dan Tanda Tangan Elektronik.

Melalui gambar di atas ini, dapat dijabarkan bahwa semakin memenuhi CIAANA, maka semakin kuat nilai kekuatan pembuktiannya. Adapun penjelasannya sebagai berikut:

2.2.3.1. Posisi lemah hanya ditempati oleh informasi elektronik sehingga sifatnya:

2.2.3.1.1. Tidak jelas siapa yang bertanggung jawab,

2.2.3.1.2. Tidak rahasia,

2.2.3.1.3. Tidak otentik,

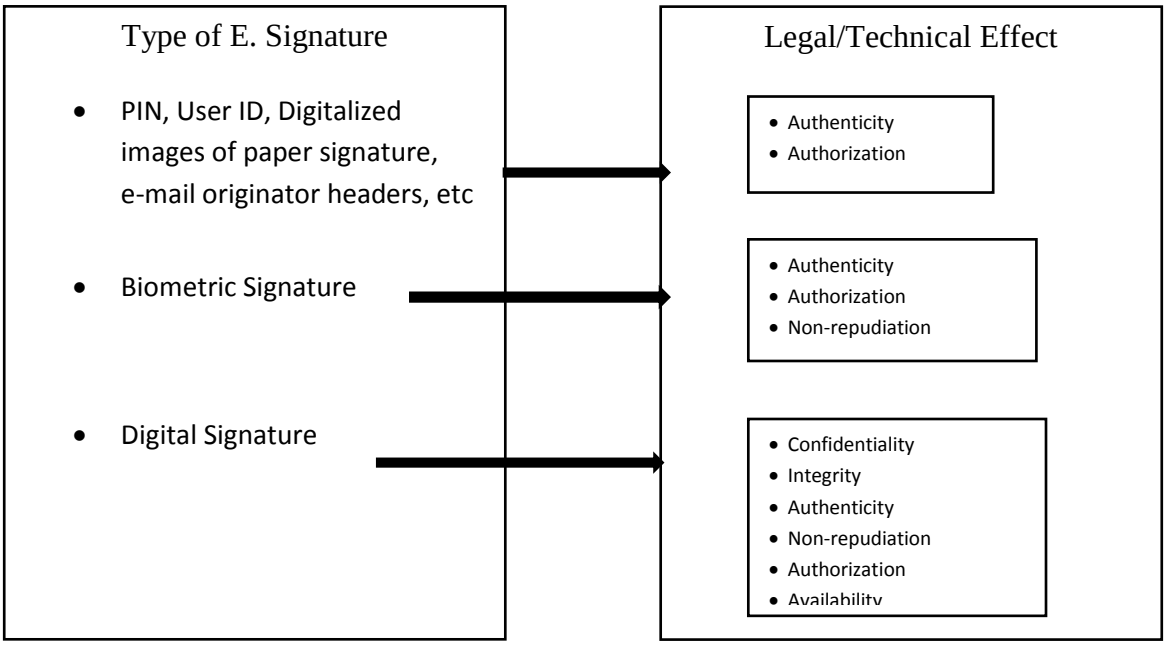
2.2.3.1.4. Tidak utuh, dan

2.2.3.1.5. Dapat ditampik.

2. Posisi *intermediate* atau menengah ditempati oleh informasi yang telah dibubuhi TTE sehingga sifatnya:
   a. Jelas siapa yang bertanggungjawab (para pihak yang melakukan TTE),
   b. Boleh jadi utuh tapi tidak belum terverifikasi sehingga belum otentik,
   c. masih dapat ditampik.
3. Posisi kuat ditempati oleh informasi yang telah dibubuhi tanda tangan digital yang tersertifikasi dan terakreditasi sehingga sifatnya:

a. Jelas siapa yang yang bertanggungjawab,
b. terverifikasi dan otentik,
c. tidak dapat ditampik.

E-Signature Weight of Evidence



Gambar 2: perbedaan bobot pembuktian beberapa jenis tanda tangan elektronik berdasarkan kriteria komunikasi yang aman[70]

Stephen Mason memperhatikan adanya perbedaan bobot nilai pembuktian terhadap tanda tangan elektronik (*Weight of Evidence*), dimana kekuatan pembuktian akan sangat ditentukan oleh karakteristik pengamanannya.[71] Semakin penuh dalam menjalani prinsip tersebut (*Confidentiality*, *Integrity*, *Authorization*, *Availability*, *Authenticity*, *Non-Repudiation*, dan *Auditability*/CIAANA), maka kekuatan pembuktian akan semakin penuh atau semakin kuat.

Menurut Sutan Remi Sjahdeini, sistem pengamanan komunikasi elektronik (*secured communication*) harus mengakomodasi kebutuhan-kebutuhan pengaman yang berkaitan dengan aspek-aspek:[72]

[70] Edmon Makarim, *Notaris dan Tanda Tangan Elektronik, Op.Cit.*, Hlm.45.
[71] *Ibid.*, Hlm 20.
[72] Sutan Remy Sjahdeini, *Sistem Pengamanan E-Commerce*, Jurnal hukum bisnis vol.18, 2002, Hlm.6.

1. *Confidentiality*

   Confidentiality menyangkut kerahasiaan data dan/atau informasi, perlindungan informasi tersebut terhadap pihak yang tidak berwenang. Informasi seharusnya dilindungi terhadap pihak luar yang tidak berwenang, terhadap *hackers* dan terhadap intersepsi atau gangguan selama transmisi melalui jaringan komunikasi sedang berlangsung. Caranya adalah dengan membuat informasi itu "tidak dapat dipahami" (*unintelligible*) oleh pihak-pihak yang tidak berwenang atau tidak bertanggung jawab itu. Untuk membuat informasi itu "tidak dapat dipahami", isi dari informasi itu harus ditransformasikan sedemikian rupa sehingga tidak dapat dipahami (tidak *decipherable*) oleh siapapun yang tidak mengetahui prosedur proses transformasi itu.

2. *Integrity*

   Integrity menyangkut perlindungan data terhadap usaha memodifikasikan data itu oleh pihak-pihak yang tidak bertanggung jawab, baik selama data itu disimpan atau selama data itu dikirimkan kepada pihak lain. Sistem pengamanan harus mampu memastikan bahwa pada waktu diterima oleh penerima, informasi itu harus muncul sama seperti ketika informasi itu disimpan atau dikirimkan. Sistem pengamanan yang dibangun harus memungkinkan untuk mengetahui apabila terhadap isi yang asli dari informasi yang dikirimkan itu telah terjadi modifikasi, tambahan atau penghapusan. Sistem tersebut juga harus dapat mencegah "dimainkannya kembali" (*re-played*) informasi itu, misalnya *fresh copy* dari data tersebut dikirimkan lagi dengan menggunakan otorisasi yang semula dipakai ketika pesan yang sesungguhnya itu dikirimkan. Oleh karena itu, diperlukan adanya suatu mekanisme yang dapat memastikan kebenaran isi pesan yang dikirimkan itu dan untuk dapat memastikan otentikasi atas pembuatan salinan dari pesan tersebut, yaitu otentikasi bahwa salinan itu sesuai dengan aslinya.

3. *Authorization*

Authorization menyangkut pengawasan terhadap akses kepada informasi tertentu. Transaksi-transaksi tertentu mungkin hanya dapat diakses oleh pihak-pihak tertentu saja, sedangkan transaksi-transaksi yang lain tidak. *Authorization* dimaksudkan untuk membatasi perbuatan oleh pihak-pihak yang tidak berwenang untuk dapat berbuat sesuatu di dalam lingkungan jaringan informasi itu. Pembatasan tersebut tergantung pada *security level* dari pihak yang bersangkutan. Pembatasan itu menyangkut sampai sejauh mana pihak yang diberi kewenangan untuk melakukan akses terhadap hal itu diberi wewenang untuk dapat melakukan hal-hal sebagai berikut:

a. Memasukan data/informasi;
b. Membaca data/informasi;
c. Memodifikasi, menambah, atau menghapus data/informasi;
d. Mengekspor atau mengimpor data/informasi;
e. Menge-*print* data/informasi.

Hak-hak istimewa tersebut dapat dikendalikan atau diawasi, baik oleh petugas tertentu atau oleh suatu unit tertentu yang ditugasi khusu untuk keperluan tersebut, dengan cara menggunakan *access control list* (ACL). ACL adalah suatu daftar yang memuat siapa-siapa saja dan tingkat kewenangan dari masing-masing orang atau pejabat tersebut untuk mengakses data itu.

4. *Availability*

Informasi yang disimpan atau ditransmisikan melalui jaringan komunikasi harus dapat tersedia sewaktu-waktu apabila diperlukan. Sistem perlindungan itu harus dapat mencegah timbulnya sebab-sebab yang dapat menghalangi tersedianya informasi yang diperlukan itu. Kesalahan-kesalahan jaringan (*network errors*), listrik mati (*power outages*), kesalahan-kesalahan operasional (*operational errors*), kesalahan-kesalahan yang bersangkutan dengan aplikasi peranti lunak yang digunakan (*software application*), masalah-masalah yang

menyangkut peranti keras (*hardware problems*), dan virus merupakan beberapa sebab yang dapat membuat informasi yang diperlukan itu menjadi tidak tersedia ketika dibutuhkan (*unavailability of information*).

5. *Authenticity*

Authenticity atau *authentication* menyangkut kemampuan seseorang, organisasi, atau komputer untuk membuktikan identitas pemilik informasi tersebut yang sesungguhnya. Semua pihak yang terlibat dalam suatu transaksi harus merasa aman dan pasti bahwa komunikasi yang terjadi melalui jaringan di antara pihak-pihak itu adalah benar, yaitu benar bahwa para pihak berhubungan dengan pihak-pihak yang sesungguhnya diinginkan dan benar mengenai informasi yang dipertukarkan di antara mereka.

Apabila suatu pesan diterima, maka penerima harus dapat memverifikasi bahwa pesan itu benar-benar dikirimkan oleh orang atau pihak yang sesungguhnya. Sebaliknya juga, harus dapat dipastikan bahwa pesan tersebut memang telah dikirimkan kepada dan telah diterima oleh pihak yang sesungguhnya dituju.

6. *Non-repudiation of origin*

Non-repudiation of origin atau *non-repudiability* menyangkut perlindungan terhadap suatu pihak yang terlibat dalam suatu transaksi atau kegiatan komunikasi di belakang hari pihak tersebut menyanggah bahwa transaksi atau kegiatan tersebut benar telah terjadi. Sistem *non-repudiation of origin* atau *non-repudiability* harus dapat membuktikan kepada pihak ketiga yang independen mengenai originalitas dan mengenai pengiriman data yang dipersoalkan itu.

Setelah suatu pesan dikirimkan kepada pihak lain, pengirim harus tidak mungkin dapat membantah bahwa dia telah mengirimkan pesan tersebut. Sebaliknya juga, penerima pesan tersebut seharusnya tidak mungkin dapat membantah bahwa yang bersangkutan telah menerima pesan tersebut.

7. *Auditability*

Data tersebut harus dicatat sedemikian rupa bahwa terhadap data itu semua syarat-syarat *confidentiality* dan *integrity* yang diperlukan telah terpenuhi, yaitu bahwa pengiriman data tersebut telah dienkripsi (*encrypted*) oleh pengirimnya dan telah didekripsi (*decrypted*) oleh penerimanya sebagaimana mestinya.

Dalam Pasal 54 Rancangan Peraturan Pemerintah Penyelenggaraan Sistem dan Transaksi Elektronik, TTE dibagi menjadi 2, yaitu:

1. Tanda Tangan Elektronik tersertifikasi
2. Tanda Tangan Elektronik tidak tersertifikasi

TTE tersertifikasi dibuat dengan menggunakan jasa penyelenggara sertifikasi elektronik sehingga dapat disebut dengan *advanced electronic signature* sedangkan TTE yang tidak tersertifikasi dibuat tanpa menggunakan jasa penyelenggara sertifikasi elektronik, dapat disebut juga dengan *ordinary signature*. TTE tersertifikasi dibagi menjadi 2, yaitu:

a. TTE yang berinduk

   Dalam TTE yang berinduk biasanya berinduk pada sertifikat yang dikeluarkan oleh *Root CA* dan badan pengawas CA pada suatu negara tertentu. Hal ini yang menentukan apakah ia dapat beroperasi di negara yang bersangkutan.

b. TTE yang tidak berinduk.

Dalam prakteknya suatu TTE juga memerlukan suatu sertifikat elektronik yang mendukung keberadaannya, sebagaimana layaknya suatu tanda tangan konvensional yang melekat pada suatu kartu tanda pengenal (contoh Kartu Tanda Penduduk/KTP) untuk melakukan verifikasi tanda tangan yang dibubuhkan.[73] Secara teknis, meskipun dilengkapi dengan sistem yang canggih untuk menciptakan keyakinan terhadap suatu TTE dan Sertifikat Elektronik, pada dasarnya hal tersebut akan berpulang lagi

[73] Edmon Makarim. *Op.Cit.*, Hlm.36.

kepada kaedah hukum nir-sangkal, yakni jika hanya dilakukan oleh kedua belah pihak yang berkomunikasi tanpa melibatkan pihak ketiga yang layak dipercaya (*Trusted Third Parties/* T3P), maka tetap saja ada peluang bagi salah satu pihak untuk melakukan penyangkalan dikemudian hari.[74] Oleh karena itu, untuk memastikan tidak dapat disangkal lagi, maka diperlukan peranan pihak ketiga sebagaimana layaknya notaris dalam penggunaan tandatangan elektronik dalam transaksi tersebut.[75] Secara teknis, fungsi ini diemban oleh CA/CSP. Jika dipertemukan antara spektrum nilai kekuatan pembuktian informasi elektronik dengan keterhubungan antara suatu Informasi Elektronik (IE) dengan TTE berikut fungsi dan peran T3P sebagai pendukungnya (termasuk peranan notaris serta perhimpunannya jika mereka berperan serta sesuai hukum nasionalnya), maka dapat disampaikan suatu catatan penting bahwa:

1. Keberadaan suatu IE yang lemah adalah informasi yang tidak jelas siapa subyek hukum yang bertanggungjawab padanya dan tidak jelas apakah informasi itu terjaga keutuhannya.
2. Keberadaan suatu IE yang cukup kuat nilai pembuktian hukumnya adalah yang melekat padanya suatu tanda tangan elektronik sebagai sistem yang mampu mengidentifikasi siapa subyek hukum yang bertanggung jawab berikut kejelasan pengamanan terhadap informasi itu sendiri (*identification & authentication/integrity*). Terhadap hal ini diberlakukan pendekatan yang minimalis yakni pendekatan kesetaraan fungsional secara “tertulis” dan “asli”.
3. Sementara suatu TTE yang mempunyai nilai pembuktian yang kurang kuat adalah TTE yang tidak melibatkan peranan suatu pihak ketiga yang layak dipercaya (*trusted third parties*) keberadaannya hanya antara para pihak yang membuat dan menerimanya.

[74] *Ibid.*
[75] *Ibid.*

4. Suatu TTE yang mempunyai nilai pembuktian yang cukup kuat adalah apabila melibatkan peranan suatu pihak ketiga yang layak dipercaya (*trusted third parties*) yang didukung dengan keberadaan suatu Sertifikat Elektronik di dalamnya (*ordinary signature*).
5. Selanjutnya, suatu Sertifikat Elektronik (*e-certificate*) yang paling kuat adalah apabila penyelenggara CSP dan *Certificate*-nya telah memenuhi akreditasi pada suatu negara dimana ia digunakan (*qualified certificate*).
6. Sementara peranan pihak T3P yang paling kuat adalah apabila mereka menyertakan fungsi dan peran notaris di dalamnya, paling tidak sebagai pemeriksa dan legalisasi identifikasi seseorang dalam proses pendaftaran dan perolehan *certificate* (RA) di dalamnya. Proses ini akan menjamin bahwa pihak yang mengajukan sertifikat adalah orang yang benar dan memastikan yang bersangkutan menerimanya secara langsung.
7. Sedangkan peranan fungsi notaris yang paling kuat dalam mendukung Transaksi Elektronik adalah apabila mereka dapat bertindak hanya sebagai RA melainkan juga memiliki kewenangan untuk membuat suatu akta secara elektronik.
8. Akhirnya fungsi dan peran Ikatan Notaris yang paling kuat adalah apabila mereka bertindak menjadi CA atau sub-CA bagi para notaris yang menjadi anggotanya.[76]

Adapun tiga pendekatan dalam pengaturan tentang TTE, khususnya melihat kekuatan pembuktian dari suatu informasi elektronik, yakni:[77]

1. Pendekatan minimalis (*minimalist approach/functional equivalent approach*)

   Pendekatan ini diperkenalkan oleh UNCITRAL *Model Law of E-commerce* (2006) dan UNCITRAL *Model Law on Electronic Signatures* (2001) yang menganut asas teknologi netral. Pendekatan

[76] *Ibid.,* Hlm.37-38.
[77] *Ibid.,* Hlm.60-73.

ini mengharapkan sistem hukum dapat mengakomodir semua jenis teknologi penyelenggaraan tanda tangan elektronik. Pendekatan ini memberikan pengakuan hukum dengan standar yang minimun untuk mengakui status hukum semua bentuk tanda tangan elektronik. Fokusnya lebih mengarah kepada persyaratan fungsional kerja dan metode otentisitas bukan kepada penyebutan teknologi tertentu. Berdasarkan pendekatan ini, tanda tangan elektronik dianggap setara dengan tanda tangan di atas kertas (*functional equivalent approach*) dengan ketentuan bahwa teknologi yang digunakan dapat berupa apa saja sepanjang dimaksudkan untuk berfungsi sebagai tanda tangan (*integrity & authenticity*), di samping adanya persyaratan tertentu terhadap syarat keandalan teknologi netral.

Ketentuan *model law* diperkuat dengan lahirnya ECC yang menyatakan secara tegas bahwa suatu komunikasi elektronik selayaknya mendapat pengakuan hukum atau tidak dapat ditampik hanya dengan alasan semata-mata bahwa bentuknya yang elektronik. Transaksi yang menggunakan komunikasi elektronik untuk kontrak internasional, berdasarkan *article* 9 ECC, tidak harus mempersyaratkan dalam suatu bentuk baku tertentu (*particular form*). Syarat tersebut meliputi:

a. *Article* 9 *section* (2) ECC, jika hukum mempersyaratkan bahwa suatu transaksi harus dilakukan secara “tertulis”, maka persyaratan tersebut dianggap terpenuhi oleh suatu komunikasi elektronik, apabila kontennya dapat diakses kembali sehingga dapat digunakan untuk referensi berikutnya,
b. *Article* 9 *section* (3) ECC, jika hukum mempersyaratkan bahwa suatu transaksi harus dilakukan secara “bertanda-tangan”, maka persyaratan tersebut dianggap terpenuhi oleh suatu komunikasi elektronik, apabila terdapat suatu metode yang dapat digunakan untuk mengidentifikasikan para pihak dan mengindikasikan adanya persetujuan para pihak, dapat dipercaya secara patut

sesuai dengan tujuan pemanfaatannya dan dapat terbukti secara faktual.

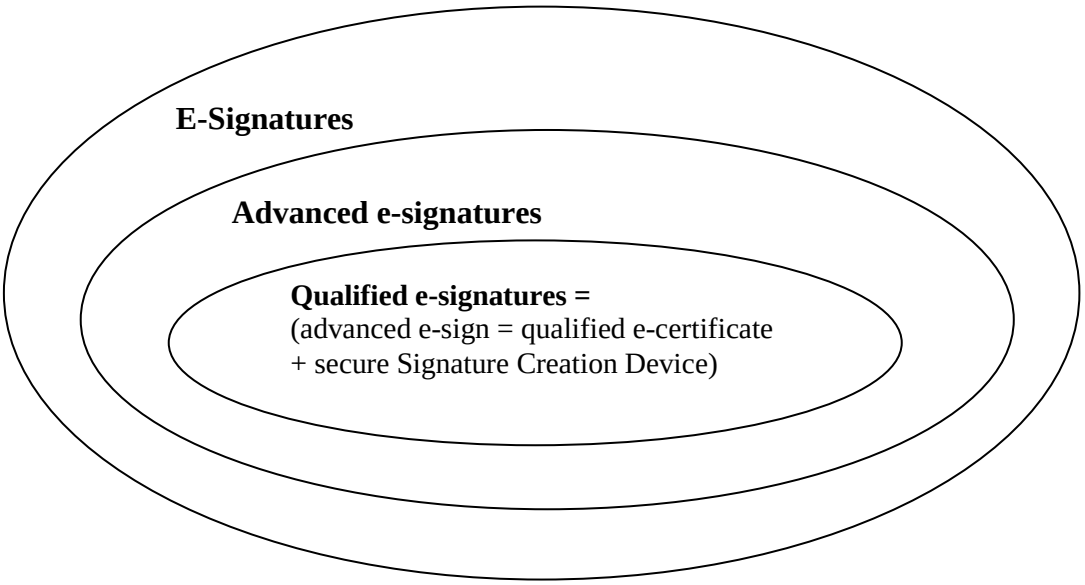
c. *Article* 9 *section* (5) ECC, jika hukum mempersyaratkan bahwa suatu transaksi harus dilakukan secara "tertulis", maka persyaratan tersebut dianggap terpenuhi oleh suatu komunikasi elektronik, apabila adanya suatu jaminan kepercayaan terhadap keutuhan informasi yang dikomunikasikan sejak bentuk awal pembuatannya sampai bentuk akhirnya dan bilamana dibutuhkan ketersediaannya, informasi elektronik tersebut dapat ditampilkan kepada pihak yang ditujunya.

2. Pendekatan dua jenjang (*two-tried approach*)

   Pendekatan ini dianut dalam komunitas eropa, khususnya dengan adanya keberadaan ECC. Dengan keberadaan *Directive* 1999/93/EC tentang *Electronic Signatures*, maka ditetapkanlah suatu titik terendah persyaratan suatu metode otentikasi elektronik dan menerima status hukum minimun tertentu serta memberikan suatu akibat hukum yang lebih besar untuk metode otentikasi elektronik tertentu yang lebih tinggi atau terakreditasi. Belanda juga menggunakan jenis pembobotan ini, paling tidak terdapat dua jenis pembobotan, yakni:[78]

   1. Tingkat yang simpel atau biasa (*ordinary*), atau
   2. Tingkat yang lebih aman (*advanced*) ataupun terakreditasi.

[78] Edmon Makarim, *Notaris dan Tanda Tangan Elektronik, Op.Cit.,* Hlm.66.



Gambar 3. Diagram Kualifikasi E-Signatures

3. Pendekatan pengaturan tanda tangan digital

   Pendekatan berbasiskan teknologi tertentu adalah paradigma pengaturan *e-signature* yang hanya merujuk kepada suatu jenis teknologi tertentu saja, yakni penggunaan tanda tangan digital dengan PKI-nya. UNCITRAL melihat adanya tiga model utama sebagai berikut:

   a. Swa-Regulasi (*self regulation*)

      Bidang usaha dan jasa otentikasi dibiarkan terbuka lebar, sementara pemerintah dapat membentuk satu atau lebih skema otentikasi dalam departemen sendiri dan organisasi terkait. Sektor swasta bebas untuk mengatur skema otentikasi, komersial atau sebaliknya, sesuai dengan tujuannya. Tidak ada kewajiban mempunyai otoritas otentikasi tingkat tinggi dan penyedia layanan otentikasi yang bertanggung jawab untuk memastikan interoperabilitas dengan penyedia jasa otentikasi lainnya. Tidak ada persyaratan perijinan (lisensi) atau persetujuan yang diperlukan pemerintah terhadap pemilihan atau pengguna teknologi oleh penyedia layanan otentikasi.

b. Pembatasan keterlibatan pemerintah (*limited government involvement*)

Pemerintah dapat memutuskan untuk mendirikan otoritas tingkat tertinggi otentikasi baik secara sukarela ataupun wajib. Penyedia layanan otentikasi tentunya merasa perlu untuk berinteroperasi dengan otoritas tingkat tinggi untuk memiliki bukti bahwa otentikasi mereka dapat diterima di luar sistem mereka sendiri. Dalam hal ini adanya syarat perijinan (lisensi) dan persetujuan terlebih dahulu dari pemerintah terhadap teknologi yang akan digunakan oleh setiap penyedia layanan otentikasi adalah suatu konsekwensi logis yang terjadi.

c. Peranan pemerintah yang (*government-led process*)

Pemerintah berhak memutuskan untuk mendirikan sebuah penyedia layanan eksklusif otentikasi pusat. Model ini lazim diterapkan dalam kontek Sistem Identitas Manajemen kependudukan (*electronic-ID*) di negara maju. Pemerintah secara langsung dapat mengakibatkan penggunaan tanda tangan elektronik menjadi aplikatif karena diterapkan dalam kehidupan sehari-hari, khususnya dalam kepentingan warga negara untuk dapat mengakses layanan publik yang diselenggarakan oleh pemerintah.

2.3. Regulasi Kriptografi dan Standar Keamanan Informasi

2.3.1. Pengertian dan Jenis Kriptografi

Pada dasarnya menjaga keamanan dan kerahasiaan suatu pesan, data ataupun informasi dengan cara mengacak pesan menjadi pesan lain yang tidak terbaca oleh yang tidak mempunyai otorisasi merupakan fungsi dari kriptografi (*cryptography*), yakni ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirimkan dapat disampaikan

kepada penerima dengan aman.[79] Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi.

Kriptografi merupakan sebuah teknik pengamanan dan sekaligus pengotentikan data yang terdiri dari 2 (dua) proses utama, yaitu enkripsi (*encryption*) dan deskripsi (*descryption*). Enkripsi adalah proses untuk mengubah pesan asli menjadi pesan yang tersandikan atau pesan yang terahasiakan. Dekripsi adalah proses untuk membalik enkripsi agar informasi tersebut dapat dibaca kembali, yaitu dengan cara mengubah pesan yang tersandikan kembali menjadi pesan pada bentuk aslinya. Secara tradisional, kriptografi dilakukan oleh pengirim dengan menggunakan kode rahasia (*secret code*) atau kunci rahasia (*secret key*) untuk melakukan enkripsi (*encryption*) terhadap informasi tersebut, yang dengan menggunakan kode rahasia atau kunci rahasia yang sama, penerima informasi tersebut melakukan dekripsi (*descryption*) terhadap informasi tersebut.[80]

Lebih lanjut, terdapat 2 (dua) jenis sistem kriptografi sebagai suatu sistem pengamanan;

1. Kriptografi Kunci Simetrik (*Symmetric Cryptosystem*)

   Kunci Simetris adalah jenis kriptografi yang paling umum digunakan. *Symmetric Cryptosystem* atau yang disebut juga *secret key cryptosystem* didasarkan pada *single secret key* yang digunakan oleh kedua belah pihak yang terlibat dalam suatu hubungan komunikasi. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu, jadi pengirim dan penerima pesan harus memiliki kunci yang sama persis sehingga sangat penting dalam sistem ini untuk memastikan bahwa tukar-menukar kunci yang digunakan harus tetap terjamin kerahasiaannya, sebab siapapun yang memiliki kunci tersebut termasuk pihak-pihak yang tidak diinginkan dapat membuat dan membongkar rahasia yang

[79] Onno W. Purbo dan Aang Arif Wahyudi, 2001, *Mengenal E-Commerce*, PT. Elex Media Komputindo, Jakarta, hal.92.
[80] *Ibid.,* Hlm.92.

tersimpan dalam pesan, data, atau informasi yang sudah tersandikan.[81] Salah satu algoritma simetris yang digunakan adalah *Data Encryption Standard* (selanjutnya disebut DES) yang mempunyai panjang kunci 64 bit.

2. Kriptografi Kunci Asimetrik/Kunci Publik (*Asymmetric Cryptosystem*)

   Asymmetric Cryptosystem atau yang disebut juga dengan sebutan *public key cryptosystem* ini mencoba menjawab permasalahan pendistribusian kunci pada teknologi kriptografi kunci simetrik. Sistem ini mendasarkan pada penggunaan sepasang kunci, yakni *private key* dan *public key*, yakni apabila suatu pesan dienkripsi dengan menggunakan *private key* dari pengirim, maka pesan tersebut hanya mungkin dideskripsi dengan menggunakan *public key* pengirim yang hanya diketahui oleh penerima, demikian juga sebaliknya.[82] Salah satu algoritma yang diaplikasikan oleh Rivest, Shamir dan Adleman, dengan membuat sebuah algoritma asimetris RSA pada tahun 1977. Sebuah kunci RSA mempunyai panjang kunci yang bervariasi mulai dari 40 bits hingga 2048 bits12.

Kapan pengiriman pesan dienkripsi oleh pengirim dengan menggunakan *private key*-nya sendiri atau kapan dideskripsi dengan menggunakan *public key* penerima adalah bergantung kepada isi dan sifat pesan yang akan dikirimkan dan bergantung pula pada bagaimana perjanjian diantara para pihak yang berkomunikasi.

Seperti yang ditunjukkan oleh namanya, *public key* dapat dan boleh diketahui oleh setiap orang, sedangkan *private key* hanya diketahui oleh pemiliknya saja. Prosedur yang digunakan untuk memperoleh kedua kunci tersebut adalah sedemikian rupa sehingga apabila salah satu kunci tersebut digunakan untuk mengenkripsi suatu pesan, hanya kunci lain pasangannya yang dapat digunakan untuk mendekripsi pesan tersebut,

[81] *Ibid.,* Hlm.95.
[82] *Ibid.*

dengan kata lain, menggunakan *private key* yang lain tidak dapat memecahkan kode tersebut. Meskipun kedua kunci tersebut berkaitan satu dengan yang lain dan meskipun *public key*-nya dapat diketahui oleh orang lain, namun tidak mungkin bagi siapapun untuk dapat mengetahui atau memperoleh *private key* yang digunakan, kecuali oleh pemiliknya sendiri, sebab dengan hanya mengetahui suatu *public key*, tidak mungkin dapat diketahui atau dipecahkan apa yang menjadi *private key* yang merupakan pasangan *public key* tersebut.[83]

Begitu sulitnya orang untuk dapat memecahkan kunci rahasia berdasarkan *public key cryptosystem* atau *asymmetric cryptosystem*, sehingga telah dianggap bahwa tidak ada 1 (satu) komputer pun yang mampu memecahkan kunci tersebut sekalipun dalam jangka waktu ribuan tahun. Memang pernah dilakukan demonstrasi, yaitu pernah dicoba sebanyak 350 (tiga ratus lima puluh) komputer yang dihubungkan melalui jaringan internet untuk mencari kombinasi yang tepat. Komputer-komputer tersebut bekerja dengan kecepatan 1 ½ (satu setengah) triliun kunci kombinasi per jam. Ternyata baru dalam waktu 320 (tiga ratus dua puluh) jam komputer-komputer tersebut berhasil menemukan kunci yang tepat.[84]

Berdasarkan penjelasan di atas, dapat diketahui berapa lama waktu dan besarnya biaya yang dibutuhkan untuk mampu memecahkan *public key* atau *asymmetric cryptosystem* tersebut. Oleh karena itu, sistem ini dianggap merupakan sistem yang paling aman untuk menjamin *confidentiality, authentication* dan *non repudiation* dari pesan yang dikirimkan.

[83] Direktorat Jenderal Perdagangan Dalam Negeri Departemen Perindustrian dan Perdagangan Jakarta dan Lembaga Kajian Hukum dan Teknologi Fakultas Hukum Universitas Indonesia, *Naskah Akademik Rancangan Undang-Undang Tentang Tanda Tangan Elektronik dan Transaksi Elektronik*, 2001, Jakarta, hal.75.

[84] *Ibid.*

Berikut cara bekerja *asymmetric cryptosystem* dengan mengaplikasikan *private key* dan *public key* berpasangan:

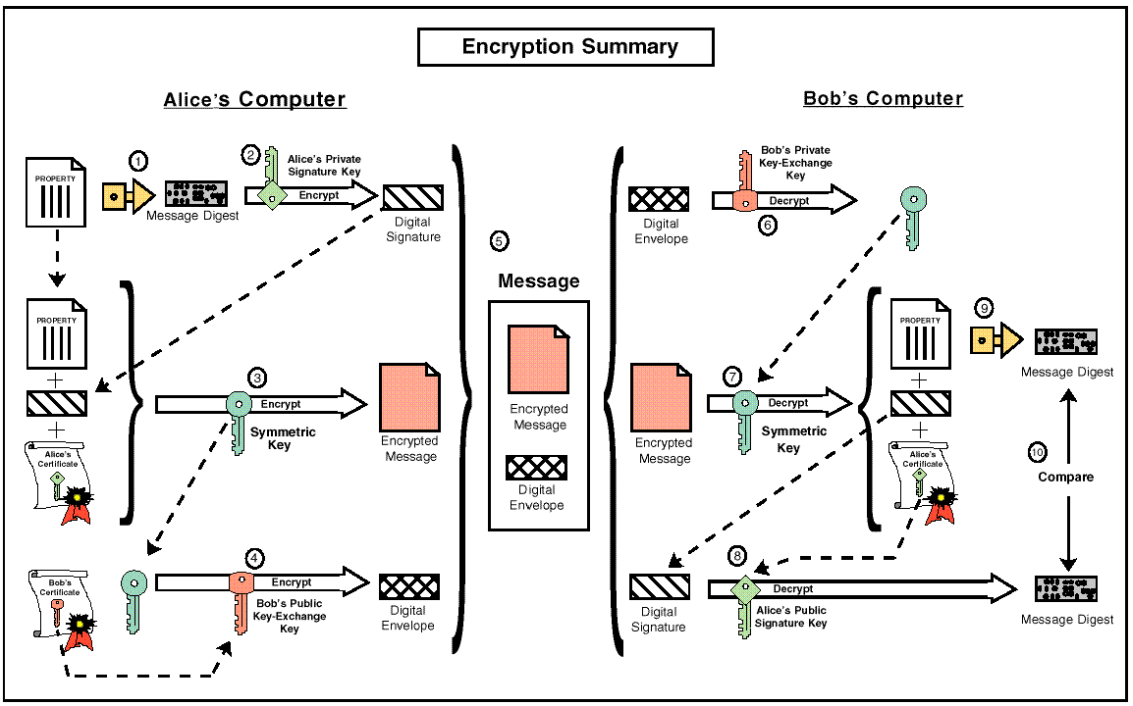
1. Cara pertama ialah melakukan enkripsi oleh pengirim dengan menggunakan *public key* penerima dan dekripsi oleh penerima dilakukan dengan menggunakan *private key* penerima;
2. Cara kedua ialah pengirim mengenkripsi pesan yang akan dikirim dengan menggunakan *private key* pengirim dan ketika penerima melakukan dekripsi pesan yang diterimanya itu, penerima melakukan dekripsi itu dengan menggunakan *public key* pengirim.[85]

Apabila pengirim menginginkan hanya penerima saja yang boleh mengetahui isi pesan yang dikirimkan, maka pengiriman pesan itu harus dilakukan dengan cara pertama, yaitu pengirim mengenkripsi pesan dengan *public key* penerima, karena pesan tersebut hanya dapat dipahami oleh penerima saja dengan cara mendekripsi pesan tersebut dengan menggunakan *private key* penerima yang hanya dimiliki oleh penerima saja. Tujuan utama dari kriptografi adalah kerahasiaan. Melalui kriptografi, penerima yang dituju yang dapat meng"*unlock*" (*decrypt*) sebuah pesan yang terenkripsi. Menjamin integritas pesan adalah hal penting lainnya dalam kriptografi, yakni integritas data dan *non-repudiation*. Tanda tangan digital menjamin bahwa pesan yang diterima adalah pesan yang sebelumnya dikirim karena *hashing value* yang diciptakan dari proses ini dienkripsikan oleh pemilik *hash* yang diciptakan oleh *author*, yakni *hash* dari pesan. Jika pesan yang diterima cocok dengan pesan yang dikirimkan, maka penerima bisa tahu bahwa pesan tersebut tidak hilang pada saat akses ke *private key* mereka, dengan asumsi bahwa kunci tersebut tetap terjaga kerahasiaannya. *Asymmetric crypthography* menjamin bahwa *author* tidak dapat menyangkal bahwa mereka menandatangani atau mengenkripsi pesan yang dimaksud ketika pesan tersebut dikirimkan.[86]

[85] *Ibid.,* Hlm. 82-83.
[86] *Ibid.,* Hlm.83.

Berkaitan dengan keamanan pesan rahasia, teknik kriptografi modern menjamin sedikitnya lima keamanan minimal, yaitu:

1. Keontentikan, penerima pesan harus mengetahui siapa pengirim pesan tersebut dan harus benar-benar yakin bahwa pesan tersebut berasal dari pengirim;
2. Integritas, penerima harus yakin bahwa pesan tersebut tidak pernah diubah atau dipalsukan oleh pihak beritikad tidak baik;
3. Kerahasiaan, pesan tersebut harus tidak dapat dibaca oleh pihak yang tidak berkepentingan;
4. Tidak dapat disangkal (*non repudiation*), pengirim tidak dapat menyangkal bahwa bukan dia yang mengirim pesan tersebut;
5. Kontrol akses, sistem kriptografi mempunyai kemampuan untuk memberikan otorisasi ataupun melarang atas setiap akses ke pesan-pesan tersebut.[87]



Gambar 4 : *encryption summary*

[87] Fairuz. *Op.Cit.*

Gambar 4 menunjukkan proses kriptografi yang terjadi dalam *digital signature*, langkah-langkah dalam melakukan enkripsi ini adalah sebagai berikut:[88]

No	Penjelasan
1	Alice menjalankan (*runs*) data yang hendak ia kirimkan, melalui algoritma satu arah (*one way algorithm*) sehingga ia mendapat suatu nilai (*value*) yang unik dari data tersebut. Nilai ini disebut message digest. Nilai adalah semacam sidik jari bagi data tersebut dan akan digunakan dalam proses yang lebih lanjut untuk meneliti keutuhan (*integrity*) dari data tersebut.
2	Alice kemudian melakukan enkripsi terhadap *messages digest* tersebut dengan menggunakan kunci privatnya sehingga ia akan mendapatkan *digital signature* dari data tersebut.
3	Kemudian, Alice membuat (*generates*) suatu kunci simetris secara acak (random) dan menggunakan kunci itu melakukan enkripsi terhadap data yang hendak ia kirimkan, tandatangan (*signature*) miliknya, dan salinan dari sertifikat digitalnya yang berisi kunci publiknya. Untuk mendekripsi data tersebut Bob membutuhkan salinan dari kunci simetris tersebut.
4	Alice harus memiliki terlebih dahulu sertifikat milik Bob, sertifikat ini berisi salinan (*copy*) dari kunci publik milik Bob. Untuk menjamin keamanan transmisi dari kunci simetris maka kunsi tersebut dienkripsi dengan menggunakan kunci publik milik Bob. Kunci yang telah dienkripsi yang dikenal sebagai amplop digital (*digital envelope*) akan dikirimkan bersama-sama dengan data yang telah dienkripsi.
5	Alice kemudian akan mengirimkan data (*message*) tersebut yang berisi data yang telah dienkripsi dengan kunci simetris, tandatangan dan

[88] Arrianto. *Op.Cit.*

	sertifikat digital, serta kunci simetris yang telah dienkripsi dengan kunci asimetris (*digital envelope*).
6	Bob menerima pesan (*messages*) dari Alice tersebut dan kemudian mendekripsi amplop digital dengan kunci prifat yang dipunyainya, ia kemudian akan mendapatkan kunci asimetris.
7	Bob kemudian menggunakan kunci simetris tersebut untuk mendekripsi data itu (*property descryption*), tandatangan Alice dan sertifikat miliknya.
8	Ia kemudian mendekripsi *digital signature* milik Alice dengan menggunakan kunci publik milik Alice, yang didapat Bob dari sertifikat milik Alice. Dari dekripsi ini akan didapatkan *message digest* dari data tersebut.
9	Bob kemudian memproses (*run*) data itu dengan menggunakan algoritma satu arah yang sama yang digunakan Alice untuk *message digest*.
10	Akhirnya Bob akan membandingkan antara *message digest* yang didapatkannya dari proses dekripsi diatas dengan *message digest* yang didapatkan dari *digital signature* milik Alice. Kalau hasil yang didapat dari perbandingan itu adalah sama maka, Bob dapat merasa yakin bahwa data tersebut tidak pernah dirusak (*altered*) selama proses transmisi dan data itu ditandatangani dengan menggunakan kunci privat milik Alice. Kalau hasil dari perbandingan itu adalah tidak sama, maka data tersebut pastilah telah diubah atau dipalsukan setelah ditandatangani.

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.[89]

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. [90]

Penggunaan tanda tangan digital memerlukan dua proses, yaitu dari pihak penandatangan serta dari pihak penerima. Secara rinci kedua proses tersebut dapat dijelaskan sebagai berikut:[91]

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 atau tidak.

Proses pembentukan dan verifikasi tanda tangan digital memenuhi unsur-unsur paling penting yang diharapkan dalam suatu tujuan legal, yaitu:

1. Otentikasi Penandatangan: Jika pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah yang telah didefinisikan, maka tanda

[89] Fairuz. *Op.Cit.*
[90] *Ibid.*
[91] *Ibid.*

tangan digital akan dapat menghubungkan atau mengasosiasikan dokumen dengan penandatangan. Tanda tangan digital tidak dapat dipalsukan, kecuali penandatangan 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 penandatangan. Tindakan ini dapat menegaskan bahwa penandatangan setuju dan bertanggung jawab terhadap isi dokumen.
4. Efisiensi: Proses pembentukan dan verifikasi tanda tangan 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.

Kelemahan yang masih menyertai teknologi tanda tangan digital adalah:[92]

1. Biaya tambahan secara institusional: Tanda tangan digital memerlukan pembentukan otoritas-otoritas yang berhak menerbitkan sertifikat serta biaya-biaya lain untuk menjaga dan mengembangkan fungsi-fungsinya.
2. Biaya langganan: Penandatangan memerlukan perangkat lunak aplikasi dan juga membayar untuk memperoleh sertifikasi dari otoritas yang berhak mengeluarkan sertifikat.

Keunggulan yang paling utama dari adanya tanda tangan digital adalah lebih terjaminnya otentikasi dari sebuah dokumen. Tanda tangan

[92] *Ibid.*

digital sangat sulit dipalsukan dan berasosiasi dengan kombinasi dokumen dan kunci privat secara unik.[93]

2.3.2. PKI (*Public Key Infrastructure*)

PKI adalah implementasi dari berbagai teknik kriptografi yang bertujuan untuk mengamankan data, memastikan keaslian data maupun pengirimnya dan mencegah adanya penyangkalan. PKI merupakan badan pengawas CA. Baik *natural* CA (pemerintah) maupun *private* CA (swasta) yang dibawahi oleh *Root* CA sehingga diperlukannya *bridge* CA agar dapat diawasi oleh badan pengawas CA ini.

Adapun Komponen-komponen PKI antara lain:[94]

1. *Root CA*

   Merupakan suatu badan teratas dari beberapa CA yang dibawahinya.

2. *Certification Authorities* (CAs)

   Suatu badan yang berwenang untuk memberikan validasi atau sertifikat digital pada kunci publik dalam suatu negara.

3. *Repository* kunci, sertifikat dan *Certificate Revocation Lists* (CRLs)

   Basis data untuk menyimpan semua data tentang kunci publik dan sertifikat kunci publik tersebut. Disamping itu terdapat *list expiry time* untuk managemen kunci bagi para pemilik kunci. CRL merupakan daftar kunci yang harus ditarik dan diganti dengan kunci yang baru. CA secara periodik mengeluarkan CRL (*Certificate Revocation List*) yang berisi nomor seri sertifikat digital yang ditarik. Sertifikat digital yang sudah kadaluarsa otomatis dianggap sudah tidak sah lagi dan dimasukkan ke dalam CRL. Dengan cara ini, maka CA tidak perlu memberitahu perubahan sertifikat digital kepada setiap orang.

[93] *Ibid.*
[94] Diiunduh pada http://www.shareilmu.com/public-key-infrastructure

4. *Management Function*

   Suatu prosedur yang digunakan untuk menjadi *guideline* dari keseluruhan proses yang ada dalam PKI.

5. *Policy Approving Authority* (PAA)

   Memberikan *guideline* untuk keseluruhan PKI dan melakukan sertifikasi kunci publik dari PCA

6. *Policy Certification Authority* (PCA)

   Memberikan *policy* untuk semua CA dan *user* yang ada pada domainnya dan melakukan sertifikasi kunci publik dari CA

7. *Organizational Registration Authority* (ORA)

   Entitas yang berperan sebagai perantara antara CA dan *user*.

Secara praktis wujud PKI adalah penggunaan sertifikat digital yaitu sebuah *file* komputer yang berisi data-data tentang sebuah *public key*, pemiliknya (*subscriber* atau CA), CA yang menerbitkannya dan masa berlakunya. PKI telah diimplementasikan dengan berbagai aplikasi seperti S/MIME, HTTPS, VPN, dll. Anda dapat melihat fitur S/MIME pada *software email* yang terkenal seperti *Outlook Express, Mozilla Mail/Thunderbird*, dan *Evolution*.[95]

Fungsi yang dilakukan PKI adalah sebagai berikut :[96]

1. Mengautentikasi identitas

   Dengan sertifikasi digital yang dikeluarkan oleh PKI maka tiap pihak dapat mengautentikasi pihak lawan dalam melakukan transaksi sehingga pihak dapat meyakini bahwa pihak yang melakukan transaksi adalah pihak yang berhak.

2. Verifikasi integritas dokumen

   Dengan adanya sertifikasi digital maka dokumen dapat diyakini tidak mengalami perubahan selama pengiriman.

[95] *Ibid.*
[96] *Ibid.*

3. Jaminan privasi

   Dengan protokol yang digunakan selama transmisi menggunakan sertifikat digital maka jalur yang digunakan dalam transmisi dipastikan aman dan tidak dapat diakses oleh pihak lain yang tidak berhak.
4. Sertifikat digital dari PKI dapat menggantikan peranan proses autentikasi *user* dalam sebuah sistem.
5. Dengan menggunakan sertifikat digital dari PKI maka suatu pihak dapat menentukan transaksi yang aman dengan menggunakan validasi kunci publik.
6. Dukungan anti penyangkalan

   Dengan adanya validasi pada sertifikat digital maka tidak mungkin untuk melakukan penyangkalan pada suatu transaksi yang telah dilakukan.

Aktifitas yang dilakukan PKI :[97]

1. Pembangkitan, pemberian sertifikat dan pendistribusian kunci,
2. Pemberian tanda tangan dan verifikasi tanda tangan,
3. Perolehan sertifikat,
4. Verifikasi sertifikat,
5. Penyimpanan sertifikat untuk penggunaan lebih lanjut,
6. Perolehan sertifikat yang sudah disimpan,
7. Laporan kehilangan kunci,
8. Pembangkitan ulang kunci yang hilang,
9. Perolehan CRL,
10. Pemberian ulang kunci dan pemberian sertifikat ulang,
11. Pelaksanaan audit terhadap kejadian, seperti permintaan pasangan kunci dan sertifikat,
12. Pengarsipan kunci.

[97] *Ibid.*

2.3.3. Penyelenggara Sertifikasi Elektronik (CA/CSP)

Sertifikat elektronik berfungsi membawa kekuatan hukum yang kuat sehingga dapat meyakinkan identitas Penandatangan. 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 UU ITE berbunyi:

1. Setiap orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan tanda tangan Elektronik.
2. Penyelenggara Sertifikasi Elektronik harus memastikan suatu tanda tangan elektronik dengan pemiliknya.
3. Penyelenggara Sertifikasi Elektronik terdiri atas:
   a. Penyelenggara Sertifikasi Elektronik Indonesia; dan
   b. Penyelenggara Sertifikat Elektronik Asing.
4. Penyelenggara Sertifikasi Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.
5. Penyelenggara Sertifikasi Elektronik Asing yang beroperasi di Indonesia harus terdaftar di Indonesia.
6. Ketentuan lebih lanjut mengenai Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Adapun kewajiban penyelenggara sertifikasi elektronik dalam menjalani tugasnya antara lain:

1. Pendaftaran

   Bagi penyelenggara untuk pelayanan publik wajib melakukan pendaftaran dilakukan sebelum sistem elektronik dilakukan publik sedangkan penyelenggara untuk non pelayanan publik (swasta) dapat melakukan pendaftaran. Pendaftaran diajukan kepada Menteri.

2. Sertifikasi

Bagi penyelenggara untuk pelayanan publik wajib memiliki sertifikat kelaikan sistem elektronik sedangkan penyelenggara untuk non pelayanan publik secara sukarela (*voluntary*).

Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud dalam Pasal 13 ayat (1) sampai dengan ayat (5) harus menyediakan informasi yang akurat jelas, dan pasti kepada setiap pengguna jasa, yang meliputi :

1. Metode yang digunakan untuk mengidentifikasikan Penanda Tangan.
2. Hal yang dapat digunakan untuk mengetahui data diri pembuat TTE, dan
3. Hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan TTE.

CA (*Certification Authority*) berkedudukan sebagai pihak ketiga yang dipercaya untuk memberikan kepastian atau pengesahan terhadap identitas dari seseorang atau pelanggan (klien CA tersebut) dengan cara menerbitkan sertifikat elektronik. Selain itu CA juga mengesahkan pasangan kunci publik dan kunci privat milik orang tersebut. Proses sertifikasi untuk mendapatkan pengesahan dari CA 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 CA, dan
3. 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 CA 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 CA semakin tinggi pula level sertifikat yang diperoleh serta semakin ketat pula persyaratan yang ditetapkan oleh CA Sebagai contoh: untuk mendapatkan suatu sertifikat yang mempunyai level kewenangan yang cukup tinggi, terkadang CA bahkan memerlukan kehadiran secara fisik si *subscriber* sehingga CA dapat memperoleh kepastian pihak yang akan memperoleh sertifikat tersebut.

Setelah persyaratan-persyaratan tersebut diuji keabsahannya maka CA 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 CA atau suatu badan lain yang berwenang untuk itu (suatu lembaga notariat). Selain untuk memenuhi sifat *integrity* dan *authenticity* dari sertifikat tersebut, CA akan membubuhkan digital *signature* miliknya pada sertifikat tersebut.[98]

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

1. Identitas CA 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.

[98] Diunduh pada *http://en.wikipedia.org/wiki/Public_key_infrastructure*

Fungsi-fungsi CA yang telah kita bicarakan di atas dapat kita golongkan sebagai berikut :

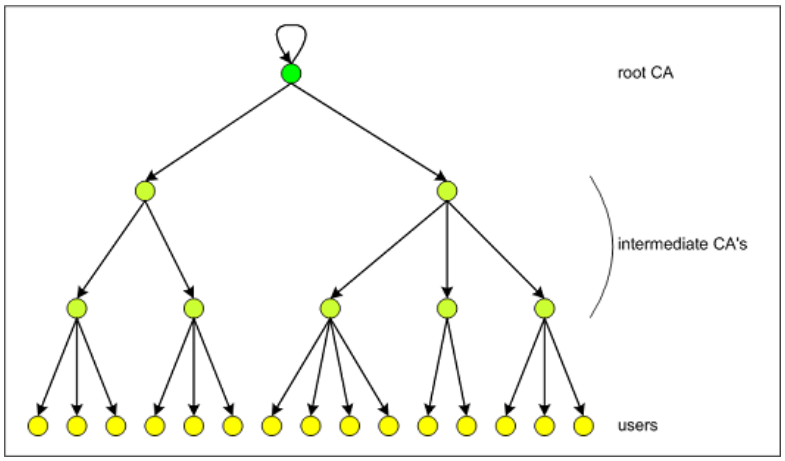
1. Membentuk hierarki bagi penandatanganan digital,
2. Mengumumkan peraturan-peraturan mengenai penerbitan sertifikat,
3. Menerima dan memeriksa pendaftaran yang diajukan.

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:

1. Penjual (*merchant*)
2. Pembeli (*buyer*)
3. *Certification Authority* (CA)
4. *Account Issuer* (penerbit rekening contoh: kartu kredit)
5. Jaringan pembayaran (contohnya Visa dan Mastercard dalam *scheme* SET)
6. *Internet Service Provider* (ISP)
7. Internet *Backbones*
8. Aspek Kontrak Perdagangan Internasional

2.3.4. *Trust* hierarki dari Sertifikat Elektronik

Kepercayaan (*Trust*) menjadi kunci utama dalam memberikan data atau informasi kepada penyelenggara sertifikasi elektronik (CA) sehingga para pengguna sertifikat elektronik dapat dengan leluasa memberikan data atau informasi tersebut kepada penyelenggara. Apabila suatu kepercayaan akan penyelenggara sertifikat elektronik tidak ada, maka akan timbul suatu keraguan dalam diri pengguna. Berdasarkan hal ini, maka model pengaturan *trust* dalam buku *Undestanding* PKI menjelaskan bahwa terdapat *multi level strict hierarchy* dan *shallow hierarchy*, dimana perbedaannya terletak pada CA di dalam posisi apa yang memberikan sertifikat elektronik kepada pengguna atau entitas terakhir.



Gambar 5 *Certificate Hierarchy*[99]

In this model, all entities in the hierarchy trust the single root CA. The hierarchy is established as follows:

1. The root CA certifies (that is, creates and signs the certificates for) zero or more CAs immediately below it.
2. Each of those CAs certifies zero or more CAs immediately below it.
3. At the second-to-last level, the CAs certify end-entities.[100]

Setiap entitas dalam hirarki (baik antara CA dan cabang non-CA) harus dilengkapi dengan salinan kunci publik *root* CA. Proses instalasi kunci publik merupakan fondasi dari proses sertifikasi untuk segala jenis komunikasi elektronik dalam model ini. Sedangkan dalam hal multi-level *strict* hirarki, segala entitas akhir disertifikasi oleh CA. Dalam hal *shallow hierarchy*, dimana tidak memiliki CA bawahan, maka *root* CA dan penerbit sertifikat adalah sama (identik) untuk semua entitas akhir.

Dalam mempercayai CA, setidaknya ada beberapa faktor yang harus diperhatikan seperti dijabarkan di dalam UNCITRAL *Model Law*

[99] Gambar *Certificate hierarchy* diunduh pada http://www.win.tue.nl/hashclash/rogue-ca/
[100] Carlisle Adams, *Op.Cit.*, Hlm.135.

on Electronic Signatures with Guide to Enactment 2001[101], sebagai berikut:

a. Keuangan dan sumber daya manusia, termasuk keberadaan aset;
b. Kualitas perangkat keras dan sistem perangkat lunak;
c. Prosedur untuk proses sertifikasi dan aplikasi untuk sertifikat dan retensi catatan;
d. Ketersediaan informasi yang diidentifikasi dalam penandatangan sertifikat dan kepada pihak yang berpontensial;
e. Keteraturan dan cakupan audit oleh badan independen;
f. Adanya deklarasi oleh negara bahwa sebuah badan akreditasi atau layanan penyedia sertifikasi telah layak atau patuh terhadap ketentuan yang ada (dalam hal ini standar kelaikannya terpenuhi), atau
g. Setiap faktor lain yang relevan.

Selain faktor-faktor di atas, sistem pengamanan merupakan hal penting yang harus diperhatikan dalam melindungi dan menambah kepercayaan konsumen terhadap CA. Dengan adanya faktor-faktor tersebut, kepercayaan konsumen kepada suatu CA menjadi lebih kuat. Sedangkan untuk CA yang memiliki faktor-faktor yang telah dijabarkan di atas, selain mendatangkan keuntungan, CA terhindar dari ancaman dan resiko yang ada sehingga dalam menjalani tugasnya mengurangi resiko dari ganti rugi yang diakibatkan CA apabila terbukti telah lalai ataupun melakukan kesalahan terhadap konsumen.

[101] *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, article 9, paragraph 1 (f), of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:*
(a) Financial and human resources, including existence of assets;
(b) Quality of hardware and software systems;
(c) Procedures for processing of certificates and applications for certificates and retention of records;
(d) Availability of information to signatories identified in certificates and to potential relying parties;
(e) Regularity and extent of audit by an independent body;
(f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or
(g) Any other relevant factor

2.4. Tanda Tangan Elektronik sebagai Alat Bukti

Dalam transaksi elektronik, alat bukti yang dapat digunakan adalah data elektronik atau digital yang ditransmisikan kedua belah pihak yang melakukan perdagangan. Adapun saksi, persangkaan, pengakuan dan sumpah, kesemuanya itu tidak mungkin dapat diajukan sebagai alat bukti karena tidak bisa didapatkan dari suatu transaksi elektronik. Apabila data atau informasi elektronik dinyatakan sebagai alat bukti dalam hal ini termasuk dalam akta otentik, maka kekuatan pembuktiannya sempurna, dimana sudah tidak memerlukan suatu penambahan pembuktian.

Sehubungan dengan pasal 1866 KUHPerdata dan pasal 164 HIR, dikenal adanya beberapa alat bukti, yakni:

1. Bukti tulisan, (Surat dan akta, baik akta otentik ataupun akta di bawah tangan),
2. Saksi-saksi,
3. Persangkaan,
4. Pengakuan, dan
5. Sumpah.

Selanjutnya dalam Pasal 1867 KUHPerdata dinyatakan bahwa bukti tulisan ada 2 (dua) jenis, yaitu:

1. Akta bawah tangan yang dibuat oleh para pihak (*private deeds*), dan
2. Akta otentik yang dibuat oleh pejabat yang berwenang (*authentic deeds*).

Kedua jenis akta tersebut mempunyai kekuatan pembuktian yang berbeda dimana akta otentik mempunyai kekuatan pembuktian yang sempurna. Selanjutnya bahkan dalam penjelasan UU No.30 tahun 2004 tentang Jabatan Notaris dinyatakan bahwa akta otentik dianggap sempurna karena ia mengandung kebenaran formil. Namun perlu juga dipahami bahwa Pasal 1869 KUHPerdata menyatakan bahwa suatu akta yang karena tidak berkuasa atau tidak cakapnya pegawai termaksud diatas, atau karena suatu cacat dalam bentuknya, tidak dapat diperlakukan sebagai akta otentik, ia hanya mempunyai

kekuatan pembuktian sebagai tulisan dibawah tangan jika akta tersebut ditandatangani oleh para pihak. Selanjutnya pada pasal 1877 KUHPerdata juga dinyatakan bahwa suatu akta otentik, yang berupa apa saja, dipersangkakan palsu, maka kekuatan eksekutorialnya dapat ditangguhkan menurut ketentuan-ketentuan dalam *Reglement* Acara Perdata.[102]

Akta otentik dipahami mempunyai 3 (tiga) aspek, yakni:

1. Kekuatan pembuktian formil, karena membuktikan antara para pihak bahwa mereka sudah menerangkan apa yang ditulis dalam akta tersebut,
2. Kekuatan pembuktian materiil karena membuktikan antara para pihak bahwa benar-benar peristiwa yang tersebut dalam akta telah terjadi, dan
3. Kekuatan pembuktian keluar yang mengikat, karena keberlakuannya juga mengikat kepada pihak ketiga diluar para pihak.[103]

Hal yang tidak jauh berbeda juga diutarakan oleh GHS Lumban Tobing, bahwa akta otentik mempunyai 3 (tiga) kekuatan pembuktian, yaitu:

1. Kekuataan pembuktian lahiriah, karena akta itu sendiri mampu membuktikan sendiri keabsahannya,
2. Kekuatan pembuktian formal karena akta tersebut dijamin kebenaran formalnya oleh pejabat sebagaimana yang telah diuraikan dalam akta, dan
3. Kekuatan pembuktian material karena akta tersebut memuat substansi atau isi yang lengkap dan dianggap kebenaran (kepastian sebagai yang sebenarnya) untuk diberlakukan kepada setiap orang atau pihak ketiga.[104]

Dalam UNCITRAL mengenai nilai hukum dari suatu rekaman elektronik (*legal value of electronic records*) karena memenuhi unsur-unsur

[102] Edmon Makarim, *Notaris dan Tanda Tangan Elektronik, Op.Cit.*, hlm.27-28.
[103] *Ibid.*, hlm.20-21.
[104] *Ibid.*, hlm.21.

tertulis (*writing*), bertanda-tangan (*signed*) dan asli (*original*).[105] Dalam Pasal 5 UU ITE juga menyatakan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti yang sah. Kecuali yang ditentukan pada Pasal 5 ayat (4) UU ITE yaitu ketentuan mengenai Informasi elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:

1. Surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan
2. Surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Penjelasan Pasal 5 ayat (4) UU ITE, bahwa surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis namun tidak terbatas pada surat berharga, surat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana dan administrasi negara.[106] Sejak dalam bentuk *original*, dokumen ataupun informasi elektronik telah diakui nilai hukumnya. Pasal 6 UU ITE telah menentukan syarat agar suatu informasi elektronik dapat disetarakan secara fungsional dengan informasi yang tertulis di atas kertas, dengan kata lain disetarakan dengan bukti tulisan, baik sebagai surat, akta bawah tangan maupun akta otentik.

Perihal persamaan atau kesetaraan tersebut dikenal dengan istilah kesetaraan fungsional (*functional equivalent approach*) yakni mempersamakan secara fungsional bahwa suatu informasi elektronik adalah sama dengan bukti tulisan jika memenuhi setidaknya tiga dasar, yakni:

1. Informasi tersebut dianggap tertulis jika ia dapat disimpan dan ditemukan kembali,

[105] *Ibid.*, hlm.24.

[106] Jusuf Patrianto Tjahjono, *Dengan Berlakunya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dan Tanda Tangan Elektronik*, 2008, www.Legal-hukum.co.id.

2. Informasi tersebut dianggap asli jika yang disimpan dan ditemukan serta dibaca kembali tidak berubah substansinya atau dengan kata lain terjamin keotentikan dan integritasnya, dan
3. Informasi tersebut dianggap bertandatangan apabila terdapat informasi yang menjelaskan adanya suatu subyek hukum yang bertanggungjawab di atasnya atau terdapat sistem otentikasi yang *reliable* menjelaskan identitas dan otorisasi ataupun verifikasi dari pihak tertentu.[107]

Dari Pasal 1 butir 4, Pasal 5 ayat (3), Pasal 6 dan Pasal 7 UU ITE dapat dikategorikan syarat formil dan materiil dari dokumen elektronik agar mempunyai nilai pembuktian, yaitu :

1. Berupa informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan, yang dapat dilihat, ditampilkan dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tulisan, suara, gambar dan seterusnya yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya;
2. Dinyatakan sah apabila menggunakan atau berasal dari Sistem Elektronik sesuai dengan ketentuan yang diatur dalam undang-undang;
3. Dianggap sah apabila informasi yang tecantum didalamnya dapat diakses, ditampilkan, dijamin keutuhannya dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Dari syarat-syarat formil dan materiil tersebut dapat dikatakan bahwa dokumen elektronik agar memenuhi batas minimal pembuktian haruslah didukung dengan saksi ahli yang mengerti dan dapat menjamin bahwa sistem elektronik yang digunakan untuk membuat, meneruskan, mengirimkan, menerima atau menyimpan dokumen elektronik adalah sesuai dengan ketentuan dalam undang-undang. Kemudian juga harus dapat menjamin bahwa dokumen elektronik tersebut tetap dalam keadaan seperti pada waktu dibuat tanpa ada perubahan apapun ketika diterima oleh pihak yang lain (*integrity*), bahwa memang benar dokumen tersebut berasal dari orang yang membuatnya

[107] Edmon Makarim, *Op.Cit.*, hlm.30.

(*authenticity*) dan dijamin tidak dapat diingkari oleh pembuatnya (*non repudiation*).

Hal ini bila dibandingkan dengan bukti tulisan, maka dapat dikatakan dokumen elektronik mempunyai derajat kualitas pembuktian seperti bukti permulaan tulisan (*begin van schriftelijke bewijs*), dikatakan seperti demikian oleh karena dokumen elektronik tidak dapat berdiri sendiri dalam mencukupi batas minimal pembuktian, oleh karena itu harus dibantu dengan salah satu alat bukti yang lain. Dan nilai kekuatan pembuktiannya diserahkan kepada pertimbangan hakim, yang dengan demikian sifat kekuatan pembuktiannya adalah bebas (*vrij bewijskracht*). Berdasarkan penalaran hukum di atas, maka dapatlah disimpulkan dokumen elektronik dalam hukum acara perdata dapat dikategorikan sebagai alat bukti persangkaan, undang-undang yang dapat dibantah (*rebuttable presumption of law*) atau setidak-tidaknya persangkaan hakim (*rechtelijke vermoden*).

Ketentuan yang ada dalam pasal-pasal tersebut menyebutkan bahwa suatu bentuk tertulis nyata (dalam hal ini segala tulisan yang dibuat berkenaan dengan kegiatan perusahaan) dapat diubah ke bentuk lain (contohnya mikrofilm atau CD) setelah sebelumnya dilakukan suatu verifikasi dan legalisasi yang dalam hal ini dilakukan oleh pimpinan perusahaan atau pejabat yang ditunjuk di lingkungan perusahaan dengan dibuatkan suatu berita acara. Setelah ada verifikasi dan legalisasi bahwa kedua bentuk dokumen tersebut isinya sama secara keseluruhan maka media hasil transformasi tersebut dan atau hasil cetaknya merupakan alat bukti yang sah.

Agar tanda tangan elektronik pada suatu informasi atau dokumen elektronik dapat mempunyai kekuatan pembuktian lebih, maka tanda tangan elektronik harus didaftarkan atau didukung oleh suatu sertifikat elektronik, diibaratkan seperti tanda tangan yang tersimpan pada KTP didaftarkan dan didukung oleh pejabat yang berwenang. Tanda tangan digital yang telah memperoleh sertifikat dari lembaga CA, maka akan lebih terjamin otentikasi dari sebuah informasi atau dokumen elektronik tersebut.

Penggunaan TTE sebagai wujud dari penggunaan suatu metode otentikasi secara elektronik menjadi suatu kebutuhan dan keniscayaan untuk memperoleh nilai kekuatan pembuktian pada tingkatan yang tinggi (*high-level*).[108]

2.5. Keamanan Informasi dalam Penggunaan Tanda Tangan Elektronik

Keamanan data atau informasi elektronik menjadi hal yang sangat penting bagi perusahaan yang menggunakan fasilitas teknologi informasi dan menempatkannya sebagai infrastruktur penting mengingat data atau informasi merupakan aset bagi perusahaan tersebut. Keamanan data atau informasi secara langsung maupun tidak langsung dapat mempertahankan kelangsungan bisnis, mengurangi resiko, mengoptimalkan *return of investment* dan bahkan memberikan peluang bisnis semakin besar. Semakin banyak informasi perusahaan yang disimpan, dikelola dan digunakan secara bersama, akan semakin besar pula resiko terjadinya kerusakan, kehilangan atau terekspos nya data dan informasi ke pihak lain yang tidak berhak. [109]

Tuntutan keamanan dalam koneksi jaringan tersebut saat ini telah lebih jauh dari sekedar pengelolaan atau pembatasan akses. Saat ini dibutuhkan sistem keamanan yang lebih kompleks dengan kesanggupan untuk mengikuti perkembangan yang ada sehingga dapat melindungi sistem dari berbagai ancaman yang mungkin timbul. Tidak semua gangguan dan ancaman datang dari pihak luar yang sengaja ingin mencuri atau merusak sistem. Gangguan dari dalam berupa kesalahan dalam menggunakan sistem atau administrasi yang tidak benar juga dapat menyebabkan kerusakan pada sistem. Oleh karena itu, sistem pada organisasi perlu dilindungi secara menyeluruh dari gangguan dan ancaman pihak luar maupun dalam.

---

[108] *Ibid.*, hlm.36.

[109] Standar Sistem Manajemen Keamanan Informasi – ISO 17799 Posted by hadiwibowo pada Februari 3, 2009.

Keamanan dalam sistem informasi memiliki pengertian sebagai berikut:[110]

1. John D. Howard, *Computer Security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.*
2. *G. J. Simons*, keamanan sistem informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.
3. *Wikipedia*, keamanan komputer atau sering diistilahkan keamanan sistem informasi adalah cabang dari teknologi komputer yang diterapkan untuk komputer dan jaringan. Tujuan keamanan komputer meliputi perlindungan informasi dan properti dari pencurian, kerusakan, atau bencana alam, sehingga memungkinkan informasi dan aset informasi tetap diakses dan produktif bagi penggunanya. Istilah keamanan sistem informasi merujuk pada proses dan mekanisme kolektif terhadap informasi yang sensitif dan berharga serta pelayanan publikasi yang terlindungi dari gangguan atau kerusakan akibat aktivitas yang tidak sah, akses individu yang tidak bisa dipercaya dan kejadian tidak terencana.

Berdasarkan pengertian di atas, keamanan informasi dalam bidang teknologi komputer ini berfungsi sebagai pencegahan atau perlindungan terhadap pencurian, penipuan, perusakan dan gangguan lainnya sehingga data atau informasi yang bersifat rahasia dan berharga terlindungi dari akibat aktivitas yang tidak sah ataupun akses individu yang tidak dapat dipercaya.

[110] *Ibid.*

Adapun pokok-pokok keamanan informasi dipilah menjadi dua area besar, yaitu:[111]

1. Keamanan informasi secara fisik

   Keamanan informasi secara fisik dapat diartikan sebagai upaya perlindungan terhadap sistem organisasi dari serangan secara fisik, yang meliputi semua elemen fisik sistem yaitu :

   a. melindungi mesin dimana aplikasi dijalankan;
   b. melindungi ruangan dimana mesin tersebut dioperasikan;
   c. melindungi gedung dimana mesin tersebut diinstal; dan
   d. melindungi daerah tempat dimana perusahaan berada.

   Elemen-elemen fisik tersebut harus dijaga dan dilindungi dari segala macam gangguan dan ancaman yang mungkin dapat terjadi. Keamanan informasi secara fisik juga termasuk mengamankan saluran komunikasi, baik komunikasi melalui kabel ataupun melalui gelombang (*wireless*). Jaringan komunikasi tersebut harus terlindung dari usaha penyadapan dan kerusakan, seperti misalnya terputusnya kabel atau lainnya.

2. Keamanan informasi secara logika

   Keamanan informasi secara logika dihubungkan pada solusi masalah-masalah keamanan TI berupa arsitektur TI, aplikasi dan prosesnya. Jaringan komunikasi harus dilindungi dengan baik tidak saja secara fisik namun juga secara logika. Sebab saat ini hampir semua organisasi dan individu terhubung ke jaringan umum internet.

   Dengan terhubung ke internet maka sumber daya di dalam komputer kita juga akan terhubung dan mungkin dapat diakses dari jauh. Karena itu sangat diperlukan perlindungan terhadap data atau informasi yang penting dan sensitif yang dimiliki agar tidak dapat diakses oleh pihak-pihak yang tidak berhak atau tidak beritikad baik. Perlindungan tersebut harus diterapkan di berbagai tingkatan keamanan. Perlindungan itu juga harus mencakup dari mulai

[111] *Ibid.*

mendesain aplikasi, membuat alur prosesnya hingga sistem penyimpanannya. Desain keamanan informasi pun perlu dibuat sedemikian rupa sehingga dapat menutup celah keamanan yang diketemukan.

a. Otentikasi

Yang dimaksud otentikasi dalam TI adalah proses mengkonfirmasi keabsahan seseorang atau sesuatu (*user*) tersebut benar sesuai dengan yang terdapat dalam *database*. Kebijakan otentikasi ini akan dapat mengendalikan *user* terhadap penggunaan sumber daya sistem dan untuk menghindari pemalsuan identitas.

Proses otentikasi meliputi pengumpulan informasi yang unik dari para *user* dan kemudian disimpan dalam sebuah *database*. Terdapat tiga mekanisme pengumpulan informasi untuk otentikasi yaitu:

(1) basis pengetahuan, seperti *username* dan *password*;

(2) basis kunci, seperti anak kunci (pintu), kunci algoritma sandi dan *smartcard*;

(3) basis biometrik, seperti sidik jari, pola suara, dan DNA.

Dalam prakteknya mekanisme pengumpulan informasi untuk otentikasi ini sering dikombinasikan untuk mendapatkan hasil otentikasi yang lebih baik. Sebagai contoh sertifikat digital yang merupakan gabungan basis pengetahuan dengan kunci, atau *voice password* yang merupakan gabungan basis pengetahuan dengan biometrik.*Username* dan *password* adalah metode otenti kasi yang paling terkenal. *User* yang akan mengakses ke sistem diminta mengetikkan *username* dan *password* untuk dicocokkan dengan *database* sistem.

Kunci (fisik) adalah sebuah objek yang dapat digunakan untuk membuktikan identitas pemegangnya. Biasanya terbuat dari logam untuk mengunci komputer atau dapat juga berupa sebuah

peralatan *hardware* yang dihubungkan dengan komputer untuk mengaktifkan program aplikasi. Atau dapat juga berupa sebuah *smartcard*. Otentikasi biometrik adalah penggunaan ciri-ciri fisik atau karakteristik tubuh sebagai sarana pencocokan identitas yang diterjemahkan kedalam sebuah nilai digital dan kemudian disimpan dalam sistem. Saat ini otentikasi biometrik telah semakin populer digunakan.

b. Otorisasi

Otorisasi adalah sebuah proses pengecekan kewenangan *user* dalam mengakses sumber daya yang diminta. Terdapat 2 (dua) metode dasar otorisasi, yaitu:

1. Daftar pembatasan akses

   Daftar pembatasan akses (*access control list*) umumnya berisi daftar *users* dengan masing-masing tugas atau kewenangannya terhadap sumber daya sistem, misalnya *use*, *read*, *write*, *execute*, *delete* atau *create*. Secara spesifik merupakan aturan yang memberikan jenis kewenangan kepada *users* atas sumber daya sistem.

2. Daftar kemampuan

   Daftar kemampuan (*capability list*) hampir sama dengan daftar pembatasan akses, namun dengan pendekatan yang berbeda yaitu dengan penitik beratan pada tugas atau kewenangannya.

Pada kenyataannya daftar pembatasan akses lebih sering digunakan karena mengelola jenis otorisasi ini relatif lebih mudah. Tugas atau kewenangan masing-masing tingkat keamanan secara spesifik berbeda, mengakibatkan berbeda *user* berbeda pula tugas atau kewenangan sehingga pembatasan akses selalu mengacu pada tugas atau kewenangan yang menyertainya.

Keamanan informasi adalah topik yang sangat luas dan kompleks, namun secara singkat keamanan informasi meliputi :[112]

a. Otentikasi atau identifikasi,
b. Pembatasan akses,
c. Kerahasiaan atau privasi,
d. Integritas data,
e. Dapat dipertanggung jawabkan (*non-repudiation*),
f. Konfigurasi atau kebijakan,
g. Keterjaminan atau pemantauan,
h. Manajemen keamanan informasi,
i. Kriptografi.

Keperluan pengembangan Keamanan Sistem Informasi memiliki tujuan sebagai berikut:[113]

a. Penjaminan integritas informasi,
b. Pengamanan kerahasiaan data,
c. Pemastian kesiagaan sistem informasi,
d. Pemastian memenuhi peraturan, hukum dan bakuan yang berlaku.

10 ancaman terhadap keamanan informasi yang sering terjadi berdasarkan urutan yang dibuat oleh *PC Magazine* edisi April 2007, yaitu:[114]

1. *Social engineering*

   Social engineering bisa juga diartikankan sebagai intelijen manusia sehingga ancaman keamanan informasi nomor satu adalah manusianya. Orang-orang yang bersentuhan dengan informasi penting dan rahasia tersebutlah yang berpotensi untuk membocorkannya. Potensi kebocoran informasi berada pada si pembuat, si pengguna, si pengolah, si pendistribusi dan/atau si penyimpan informasi. Kebocoran informasi akibat kegiatan sosial ini kadang disengaja untuk maksud tertentu, namun lebih sering

[112] *Ibid.*
[113] *Ibid.*
[114] *Ibid.*

tidak disengaja akibat orang tersebut terpancing dalam suatu pembicaraan atau kegiatan atau argumen tertentu atau *blackmail*.

2. *Identity theft*

   Di kehidupan sehari-hari, tidak mungkin seseorang berjalan di muka umum dengan topeng wajah orang lain tanpa diketahui. Namun di dunia digital hal tersebut dapat dilakukan dengan mudah. *Identity theft* atau pencurian informasi tentang identitas kita dapat dilakukan melalui komputer *off-line*, jaringan LAN dan internet maupun melalui transaksi-transaksi dikehidupan sehari-hari. Saat ini hipnotis dapat juga dimasukkan sebagai salah satu cara pencurian identitas. Motif pencurian identitas biasanya adalah uang, namun tidak tertutup kemungkinan motif lain yang bersifat pribadi, politik ataupun bisnis.

3. *Spyware* dan *trojans*

   Spyware dan *trojan horse* adalah program komputer yang biasanya tanpa sengaja terinstal untuk melakukan perusakan, penyalinan dan/atau pengintipan aktifitas sebuah komputer, sehingga segala aktifitas kita saat menggunakan komputer dapat dipantau, di-*copy* atau didalangi dari tempat lain. *Spyware* dan *trojans* biasanya terinstal karena ketidak-telitian pengguna komputer saat meng-klik suatu *pop-up* atau *browsing* internet.

4. Virus dan *worm*

   Virus dan *worm* adalah sebuah program komputer aktif yang biasanya tersembunyi dan membahayakan karena bersifat merusak komputer. Virus dapat menginfeksi program komputer lain dan/atau *file* data serta dapat terdistribusi ke komputer lain dengan membonceng pendistribusian *file* atau program lain.

5. *Adware*

   Adware adalah kependekan dari *advertising software*, yaitu sebuah program yang dibuat untuk mengiklankan sesuatu yang dapat secara otomatis tampil dalam web *browser* atau *pop-up*.

Adware bisa ter-*download* tanpa sengaja bila kita tidak teliti saat meng-*klik* iklan yang tampil dalam sebuah *pop-up*.

6. *Web exploits*

   Terkadang kita mendapati sebuah *website* yang didalamnya berisi kode-kode jahat (*malicious codes*) yang dapat mengeksploitasi lubang-lubang keamanan dalam sistem operasi dan program yang digunakan dalam komputer kita. Dengan hanya dengan mengunjugi situs tersebut, komputer kita dapat terinfeksi atau dirusak olehnya.

7. *Hacker attack*

   Hacker adalah seseorang atau beberapa orang yang ahli dan mengetahui seluk beluk komputer baik *software, hardware*, keamanan atau jaringannya. *Hacker* sering dikonotasikan sebagai penjahat di dunia komputer. Namun sesungguhnya tidak semua *hacker* melakukan kejahatan, terdapat pula *hacker* yang memang berfungsi sebagai peneliti dan pengembang dengan cara menelusuri lubang-lubang keamanan sebuah *software* atau jaringan komputer.

8. *Wireless attack*

   Dengan kehadiran prosesor dan *software* sistem operasi terbaru, teknologi *wireless* telah mulai menjadi "barang biasa". *Wireless* sangat menguntungkan dari segi problem pemasangan kabel dan kabel yang semrawut. Namun bila tidak hati-hati, seseorang dalam jangkauan area *wireless* tersebut dapat "mencuri" *bandwidth* kita. Bahkan orang tak dikenal tersebut dapat menjelajahi komputer dalam jaringan *wireless* tersebut, sebab orang tak dikenal itu berada didalam jaringan.

9. *Phishing mail*

   Phising mail adalah sebuah email yang seolah-olah dikirim dari bank tempat kita menyimpan uang, dari situs tempat kita membeli barang secara *on-line* dan lain-lain yang seupa dengan

hal seperti itu. Bila kita *log-in* kedalam situs gadungan tersebut maka situs itu akan mencuri *username* dan *password* yang akan merugikan kita.

10. *Spam mail*

Spam mail atau *junk mail* atau *bulk mail* biasanya berupa *e-mail* yang dikirim secara serentak ke beberapa alamat yang berisi pesan penawaran, tipuan dan lain-lain yang biasanya kurang berguna bagi penerimanya.

Ada beberapa hal yang harus diperhatikan dalam menghindari ancaman atau resiko tersebut, yaitu:

a. jangan gunakan program yang diberikan oleh orang yang tidak dikenal;
b. bacalah peringatan keamanan yang muncul sebelum meng-*klik*-nya;
c. gunakan *password* dengan benar;
d. gunakan program *firewall, antivirus, antispyware, antispam* yang baik dan selalu diperbaharui;
e. *back-up file-file* penting dalam sebuah media eksternal dan simpan ditempat yang aman;
f. berhati-hatilah saat meng-*klik* sebuah situs yang dirujuk dalam sebuah *e-mail*; serta
g. gunakan sistem penyandian yang baik untuk melakukan koneksi *wireless* ataupun menyimpan dan mendistribusikan data.

Apabila ancaman ini dihiraukan, konsekuensi yang didapat antara lain:

1. Pencurian data atau informasi baik identitas, *file-file* penting, dan sebagainya,
2. Penyalahgunaan data atau informasi tersebut sehingga berdampak di kemudian hari. Bagi penyelenggara CA hal ini dapat berdampak pada tanggung jawabnya sebagai CA

yang seharusnya melindungi data atau informasi yang diberikan konsumennya kepada CA tersebut.

3. Perusakan program atau sistem elektronik yang seharusnya bekerja sebagaimana mestinya.

Ancaman atau resiko ini seharusnya dijaga oleh setipa individu yang menggunakan sistem elektronik itu sendiri dan juga penyelenggara CA dengan memperketat sistem pengamanan serta manajemen yang baik dalam menjalankan fungsinya, sehingga terhindar dari bentuk-bentuk ancaman yang dapat merugikan konsumen maupun CA itu sendiri. Ancaman dan resiko yang ditimbulkan akibat kegiatan pengelolaan dan pemeliharaan data atau informasi menjadi alasan disusunnya standar sistem manajemen keamanan informasi yang salah satunya adalah ISO 17799. Penyusunan standar ini berawal pada tahun 1995, dimana sekelompok perusahaan besar seperti *Board of Certification, British Telecom, Marks & Spencer, Midland Bank, Nationwide Building Society, Shell* dan *Unilever* bekerja sama untuk membuat suatu standar yang dinamakan *British Standard 7799* (BS 7799).[115] Pada tahun 2000, *International Organization of Standardization* (ISO) dan *International Electro-Technical Commission* (IEC) mengadopsi BS 7799 Part 1 dan menerbitkannya sebagai standar ISO/IEC 17799 tahun 2000 yang diakui secara internasional sebagai standar sistem manajemen keamanan informasi. ISO 17799 meliputi 10 klausula pengendalian (10 *control clauses*), 36 sasaran pengendalian (36 *control objectives*) dan 127 pengendalian keamanan (127 *controls securiy*).[116]

[115] BS 7799 terdiri dari beberapa bagian yaitu : ***Part 1***, *The Code of Practice for Information Security Management*. ***Part 2***, *The Specification for Information Security Management Systems* (ISMS).

[116] *Ibid.*

Pengendalian adalah cara yang dipilih untuk menyingkirkan atau meminimalkan risiko ke level yang dapat diterima. Berikut adalah penjabaran 10 klausula pengendalian :[117]

1. Kebijakan Pengamanan *(Security Policy)*, mengarahkan visi dan misi manajemen agar kelangsungan organisasi dapat dipertahankan dengan mengamankan dan menjaga integritas atau keutuhan data atau informasi penting yang dimiliki oleh perusahaan. Kebijakan pengamanan sangat diperlukan mengingat banyaknya masalah-masalah non teknis seperti penggunaan *password* oleh lebih dari satu orang yang menunjukan tidak adanya kepatuhan dalam menjalankan sistem keamanan informasi. Kebijakan pengamanan ini meliputi aspek infratruktur dan regulasi keamanan informasi.

   Hal pertama dalam pembuatan kebijakan keamanan adalah dengan melakukan inventarisasi data-data perusahaan. Selanjutnya dibuat regulasi yang melibatkan semua departemen sehingga peraturan yang akan dibuat tersebut dapat diterima oleh semua pihak. Setelah itu rancangan peraturan tersebut diajukan ke pihak direksi untuk mendapatkan persetujuan dan dukungan agar dapat diterapkan dengan baik.
2. Pengendalian Akses Sistem (*System Access Control)*, mengendalikan atau membatasi akses *user* terhadap informasi-informasi dengan cara mengatur kewenangannya, termasuk pengendalian secara *mobile-computing* ataupun *tele-networking*. Mengontrol tata cara akses terhadap informasi dan sumber daya yang ada yang meliputi berbagai aspek seperti :
   a. Persyaratan bisnis untuk kendali akses;
   b. Pengelolaan akses *user* (*User Access Management*);
   c. Kesadaran keamanan informasi (*User Responsibilities*);
   d. Kendali akses ke jaringan (*Network Access Control*);

[117] *Ibid.*

e. Kendali akses terhadap sistem operasi (*Operating System Access Control*);
f. Pengelolaan akses terhadap aplikasi (*Application Access Management*);
g. Pengawasan dan penggunaan akses sistem (*Monitoring System Access and Use*); dan
h. *Mobile Computing* dan *Telenetworking.*

3. Pengelolaan Komunikasi dan Kegiatan (*Communication and Operations Management*), menyediakan perlindungan terhadap infrastruktur sistem informasi melalui perawatan dan pemeriksaan berkala, serta memastikan ketersediaan panduan sistem yang terdokumentasi dan dikomunikasikan guna menghindari kesalahan operasional. Pengaturan tentang alur komunikasi dan operasi yang terjadi meliputi berbagai aspek, yaitu:
   a. Prosedur dan tanggung jawab operasional;
   b. Perencanaan dan penerimaan sistem;
   c. Perlindungan terhadap *software* jahat (*malicious software*);
   d. *Housekeeping*;
   e. Pengelolaan *Network*;
   f. Pengamanan dan Pemeliharaan Media; dan
   g. Pertukaran informasi dan *software.*
4. Pengembangan dan Pemeliharaan Sistem (*System Development and Maintenance*), memastikan bahwa sistem operasi maupun aplikasi yang baru diimplementasikan mampu bersinergi melalui verifikasi dan validasi. Penelitian untuk pengembangan dan pemeliharaan sistem meliputi berbagai aspek, seperti : persyaratan pengamanan sistem, pengamanan sistem aplikasi, penerapan kriptografi, pengamanan file sistem dan pengamanan pengembangan dan proses pendukungnya.
5. Pengamanan Fisik dan Lingkungan (*Physical and Environmental Security*), mencegah kehilangan dan/atau kerusakan data yang

diakibatkan oleh lingkungan secara fisik, termasuk bencana alam dan pencurian data yang tersimpan dalam media penyimpanan atau dalam fasilitas penyimpan informasi yang lain. Pengamanan fisik dan lingkungan ini meliputi aspek, yaitu: pengamanan area tempat informasi disimpan, pengamanan alat dan peralatan yang berhubungan dengan informasi yang akan dilindungi dan pengendalian secara umum terhadap lingkungan dan *hardware* informasi.

6. Penyesuaian (*Compliance*), memastikan implementasi kebijakan-kebijakan keamanan selaras dengan peraturan dan perundangan yang berlaku, termasuk perjanjian kontrak melalui audit sistem secara berkala. Aspek-aspek yang diperlukan untuk membentuk prosedur dan peraturan, yaitu: penyesuaian dengan persyaratan legal, peninjauan kembali kebijakan pengamanan dan penyesuaian secara teknis serta pertimbangan dan audit sistem.
7. Keamanan personel/sumber daya manusia (*Personnel Security*), upaya pengurangan resiko dari penyalahgunaan fungsi dan/atau wewenang akibat kesalahan manusia (*human error*), manipulasi data dalam pengoperasian sistem serta aplikasi oleh *user*. Kegiatan yang dilakukan diantaranya adalah pelatihan-pelatihan mengenai kesadaran informasi (*security awareness*) agar setiap *user* mampu menjaga keamanan data dan informasi dalam lingkup kerja masing-masing. *Personnel Security* meliputi berbagai aspek, yaitu: *Security in Job Definition and Resourcing*, pelatihan-pelatihan dan *Responding to Security Incidens and Malfunction.*
8. Organisasi Keamanan (*Security Organization*), memelihara keamanan informasi secara global pada suatu organisasi atau instansi, memelihara dan menjaga keutuhan sistem informasi internal terhadap ancaman pihak eksternal, termasuk pengendalian terhadap pengolahan informasi yang dilakukan oleh pihak ketiga

(*outsourcing*). Aspek yang terlingkupi, yaitu: keamanan dan pengendalian akses pihak ketiga dan *Outsourcing*

9. Klasifikasi dan pengendalian aset (*Asset Classification and Control*), memberikan perlindungan terhadap aset perusahaan yang berupa aset informasi berdasarkan tingkat perlindungan yang telah ditentukan. Perlindungan aset ini meliputi *accountability for Asset* dan klasifikasi informasi.
10. Pengelolaan Kelangsungan Usaha (*Business Continuity Management*), siaga terhadap resiko yang mungkin timbul didalam aktivitas lingkungan bisnis yang bisa mengakibatkan ”*major failure*” atau resiko kegagalan sistem utama ataupun ”*disaster*” atau kejadian buruk yang tak terduga, sehingga diperlukan pengaturan dan pengelolaan untuk kelangsungan proses bisnis, dengan mempertimbangkan semua aspek dari *business continuity management.*

Membangun dan menjaga keamanan sistem manajemen informasi akan terasa jauh lebih mudah dan sederhana dibandingkan dengan memperbaiki sistem yang telah terdisintegrasi. Penerapan standar ISO 17799 akan memberikan benefit yang lebih nyata bagi organisasi bila didukung oleh kerangka kerja manajemen yang baik dan terstruktur serta pengukuran kinerja sistem keamanan informasi, sehingga sistem informasi akan bekerja lebih efektif dan efisien.

Tanda tangan yang semula hanya dilakukan secara konvensional telah mengalami pergeseran sehingga dapat dilakukan secara elektronik. Otentikasi dan verifikasi menjadi fungsi utama dalam tanda tangan elektronik. Dalam proses ini terlihat bahwa bobot pembuktian dari tanda tangan elektronik itu sendiri minimal mengakomodir *secured communication* (CIAANA). Semakin penuh CIAANA pada sebuah tanda tangan mengakibatkan tanda tangan elektronik tersebut sulit dibantah atau disangkal. Dalam memenuhi *secured communication* , maka diperlukan pihak lain yang berwenang (CA). Sebagai penyelenggara sertifikasi elektronik, CA sendiri

memikul tanggung jawab yang besar dalam menjaga dan melindungi data atau informasi yang diberikan kepadanya, sehingga diperlukan pengendalian atau manajemen yang baik dalam menjalankan tugasnya.

BAB III

Tanggung Jawab Hukum Penyelenggara Tanda Tangan Elektronik

3.1. Tanggung Jawab Penyelenggara Sistem Elektronik

Penyelenggara sistem elektronik tidak lain adalah penyelenggara negara, orang, badan usaha, dan/atau masyarakat yang memanfaatkan sistem elektronik misalnya untuk pelayanan publik. Setiap penyelenggara negara, orang, badan usaha dan/atau masyarakat yang memanfaatkan sistem elektronik harus tunduk pada ketentuan dalam UU ITE, diantaranya tidak melakukan perbuatan menyebarkan informasi elektronik yang dilarang, seperti pornografi, perjudian, penipuan, pengancaman, isu atau berita yang tidak benar adanya dan tindakan negatif lainnya. Sedangkan bagi yang memanfaatkan sistem elektronik ini dihimbau untuk tidak melakukan perbuatan tanpa hak seperti merusak sistem elektronik, memanipulasi informasi, menyadap informasi milik orang lain serta melakukan aktivitas-aktivitas yang merugikan yang tidak dapat dipertanggungjawabkan.

Setiap penyelenggara bertanggungjawab terhadap sistem elektronik yang diselenggarakannya kecuali berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan dan/atau kelalaian pihak pengguna sistem elektronik. Seperti halnya pihak bank bertanggungjawab terhadap sistem elektronik berupa ATM yang diselenggarakannya. Ketika diketahui adanya *hacker* yang menyerang sistem elektronik itu sehingga transaksi elektronik pun terganggu, maka pihak bank bertanggungjawab untuk memulihkan kembali sistem elektronik itu dan melaporkan ke pihak berwajib atas serangan tersebut sehingga pihak berwajib dapat melakukan penyidikan untuk mencari bukti-bukti dan pelakunya.

Untuk memastikan pemanfaatan sistem elektronik mendukung tujuan penyelenggaraan pemerintahan, maka penyelenggaraan sistem elektronik instansi pemerintah harus memperhatikan aspek efisiensi penggunaan sumber daya dan aspek pengelolaan risiko, aspek akurasi dan integritas data atau

informasi serta aspek auditabilitas. Atas dasar tersebut, Kementerian Kominfo saat ini sedang menyusun Rancangan Peraturan Menteri Kominfo tentang Pedoman Umum Audit Sistem Elektronik Penyelenggara Pelayanan Publik, yang melalui siaran pers ini dilakukan uji publik sejak tanggal 26 Mei s/d. 4 Juni 2012.[118] Beberapa hal penting yang diatur dalam RPM ini adalah sebagai berikut:

1. Setiap penyelenggara pelayanan publik (setiap institusi penyelenggara negara, korporasi, lembaga independen yang dibentuk berdasarkan undang-undang untuk kegiatan pelayanan publik, dan badan hukum lain yang dibentuk semata-mata untuk kegiatan pelayanan publik) harus menyelenggarakan sistem elektronik (serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan Informasi Elektronik) secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya.
2. Untuk menjamin penyelenggara pelayanan publik menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab sebagaimana dimaksud harus dilakukan audit sistem elektronik (proses sistematis mengumpulkan dan mengevaluasi bukti untuk menentukan secara independen dan obyektif apakah suatu sistem elektronik atau sistem informasi telah dapat melindungi aset, menjaga integritas data dan memungkinkan tujuan organisasi tercapai secara efektif dengan menggunakan sumber daya secara efisien).
3. Audit sistem elektronik sebagaimana dimaksud dilakukan terhadap penyelenggara pelayanan publik untuk mengevaluasi:
    a. kepatuhan penyelenggaraan sistem elektronik;

[118] Siaran Pers No. 44/PIH/KOMINFO/5/2012 tentang Uji Publik RPM Pedoman Umum Audit Sistem Elektronik Penyelenggara Pelayanan Publik Sabtu, 26 Mei 2012 11:27 am | gatot_s | http://kominfo.go.id/siaran_pers/detail/2967/Siaran+Pers+No.+44-PIH-KOMINFO-5-2012+tentang+Uji+Publik+RPM+Pedoman+Umum+Audit+Sistem+Elektronik+Penyelenggara+Pelayanan+Publik.

b. keamanan sistem elektronik; dan/atau
c. kinerja penyelenggaraan sistem elektronik.

4. Kepatuhan penyelenggaraan sistem elektronik sebagaimana dimaksud merupakan pemenuhan terhadap:
    a. ketentuan peraturan perundang-perundangan terkait dengan sistem dan transaksi elektronik; dan
    b. ketentuan internal, standar, dan prosedur yang terkait dengan penyelenggaraan sistem elektronik untuk layak dan dapat diaudit.
5. Keamanan sistem elektronik sebagaimana dimaksud merupakan sarana pengendalian atas penyelenggaraan sistem elektronik yang bertujuan untuk menjaga:
    a. kerahasiaan data dan informasi;
    b. integritas data dan informasi; dan
    c. ketersediaan data dan informasi.
6. Kinerja penyelenggaraan sistem elektronik sebagaimana dimaksud merupakan sarana pengendalian atas penyelenggaraan sistem elektronik yang bertujuan untuk menjamin:
    a. keandalan sistem elektronik;
    b. efektifitas sistem elektronik;dan
    c. efisiensi sistem elektronik.
7. Penyelenggara pelayanan publik yang menyelenggarakan sistem elektronik wajib:
    a. menyediakan data dan informasi catatan kegiatan dan penyimpanan, dan arsip data secara lengkap yang menjadi media kontrol operasional untuk disimpan secara independen bebas dari kemungkinan gangguan akurasi;
    b. menyampaikan informasi yang dibutuhkan terkait dengan pelaksanaan audit penyelenggaraan sistem elektronik; dan
    c. memberikan akses terhadap sistem elektronik yang diaudit.

8. Penyampaian informasi dan pemberian akses sebagaimana dimaksud dilakukan sesuai ketentuan peraturan perundang-perundangan dan bebas dari kemungkinan kebocoran informasi tanpa dijejaki selama proses penyampaian maupun pemberian akses.[119]

Setiap penyelenggara sistem elektronik memiliki persyaratan minimum dalam mengoperasikan sistem elektroniknya. Adapun persyaratan minimun tersebut termaktub dalam pasal 16 ayat 1 UU ITE yang terdiri dari 5 (lima) persyaratan, yaitu:

1. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan;
2. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut;
3. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut;
4. 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
5. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan dan kebertanggungjawaban prosedur atau petunjuk.

Tanggung jawab penyelenggara sistem elektronik sendiri tertuang pada pasal 15 ayat 1 dan 2 UU ITE yang berbunyi:

1. Setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal[120] dan aman[121] serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya[122].

---

[119] *Ibid.*

[120] Andal artinya sistem elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya.

[121] Aman artinya sistem elektronik terlindungi secara fisik dan nonfisik.

[122] Beroperasi sebagaimana mestinya artinya sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya.

2. Penyelenggara sistem elektronik bertanggung jawab[123] terhadap penyelenggaraan sistem elektroniknya.

Berdasarkan pasal 15 dan 16 UU ITE ini dianut prinsip praduga harus bertanggung jawab (*presumed liability*) kepada pelaku usaha dimana mereka bertanggung jawab secara hukum. Namun adanya pengecualian pada ayat 3 pasal 15 yang menyatakan bahwa penyelenggara sistem elektronik bebas dari tanggung jawabnya apabila dapat dibuktikan bahwa adanya keadaan memaksa, kesalahan, dan/atau kelalaian dari pihak pengguna sistem elektronik itu sendiri. Dalam prakteknya, kewajiban pembebanan pembuktian terhadap adanya kesalahan sistem tentunya tidak dapat dibebankan kepada pengguna karena mereka tidak mempunyai akses ke dalam untuk dapat melakukan pembuktian tersebut. Oleh karena itu, berdasarkan Pasal 35 UU ITE pengguna hanya cukup membuktikan bahwa bukti awal yang dimilikinya tidak merupakan hasil rekayasanya sendiri.[124]

Penyelenggaraan sistem elektronik diatur pula di dalam Rancangan Peraturan Pemerintah (RPP) Penyelenggaraan Sistem dan Transaksi Elektronik. Berdasarkan RPP ini, penyelenggara sistem elektronik memiliki kewajiban dan tanggung jawab sebagai berikut:

1. Penyelenggara sistem elektronik wajib melakukan pendaftaran yang diajukan kepada Menteri (Pasal 5);
2. Baik dalam hal pengaturan perangkat keras dan perangkat lunak wajib memenuhi persyaratan dan memperoleh sertifikasi kelaikan Menteri (Pasal 6, 7 dan 8);
3. Tenaga ahli yang digunakan penyelenggara sistem elektronik wajib memiliki sertifikat keahlian (Pasal 10);
4. Penyelenggara sistem elektronik wajib menjamin tata kelola sistem elektronik dengan baik serta menerapkan manajemen risiko terhadap kerusakan atau kerugian yang ditimbulkan (Pasal 12, 13, 14, 16 dan 17);

[123] Bertanggung jawab artinya subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggaraan sistem elektronik tersebut.

[124] Edmon Makarim, *Op.Cit.*, hlm.131.

5. Penyelenggara sistem elektronik wajib menjaga rahasia data pribadi yang dikelolanya (Pasal 15);
6. Penyelenggara sistem elektronik wajib melakukan pengamanan terhadap seluruh kegiatan atau komponen dari sistem elektronik itu sendiri (Pasal 18,19 dan 20);
7. Penyelenggara sistem elektronik wajib menjaga keutuhan, kerahasiaan, keautentikan, keteraksesan, ketersediaan dan dapat ditelusurinya suatu informasi dan/atau dokumen elektronik yang terkait dengannya (Pasal 21,22 dan 23);
8. Penyelenggara wajib melakukan edukasi kepada pengguna sistem elektronik (Pasal 24);
9. Penyelenggara wajib menyampaikan informasi kepada pengguna (Pasal 25);
10. Penyelenggara wajib menyediakan fitur yang sesuai dengan karakteristik sistem elektronik yang digunakannya (Pasal 26);
11. Penyelenggara wajib melindungi pelanggannya dan masyarakat luas dari kerugian yang ditimbulkan oleh sistem elektronik yang dikelolanya (Pasal 27);
12. Penyelenggara sistem elektronik wajib menyediakan personel yang terlatih dan bertanggungjawab terhadap pengamanan dan perlindungan sarana dan prasarana sistem elektronik (Pasal 28 dan 29);
13. Penyelenggara wajib memberikan informasi atas permintaan penyidik untuk tindak pidana tertentu (Pasal 30);
14. Penyelenggara wajib memiliki sertifikat kelaikan sistem elektronik yang diakui Menteri (Pasal 31 dan 32).

Dalam buku Carlisle Adams dan Steve Lyoyd yang berjudul *Understanding Public Key Infrastructure*, menyatakan bahwa: "*CA is obligated to:*

1. *use trustworthy system,*
2. *disclose its practices and procedures,*

3. *properly identify a prospective applicant for a certificate,*
4. *publish issued certificates in a respository,*
5. *suspend and/or revoke certificate,*
6. *make warranties to persons using the certificate to verify digitally signed messages."*[125]

Untuk meningkatkan keamanan dalam penyelenggaraan sistem elektronik, maka penyelenggara wajib menggunakan sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik. Penyelenggara sertifikat elektronik sendiri berfungsi membawa kekuatan hukum yang kuat sehingga dapat meyakinkan identitas penandatangan. Selain itu, kewajiban penyelenggara sertifikasi elektronik tertuang dalam Pasal 14 UU ITE yang menyatakan bahwa penyelenggara sertifikasi elektronik harus menyediakan informasi[126] yang akurat jelas, dan pasti kepada setiap pengguna jasa, yang meliputi :

1. Metode yang digunakan untuk mengidentifikasikan Penanda Tangan.
2. Hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda Tangan Elektronik, dan
3. Hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik.

Penyelenggaraan sertifikasi elektronik diatur pula di dalam Pasal 63 ayat 1 RPP, adapun kewajibannya sebagai berikut:

"Penyelenggara sertifikasi elektronik wajib melakukan:

a. pendaftaran dan pemeriksaan calon pemilik dan/atau pemegang sertifikat elektronik,
b. penerbitan sertifikat elektronik,
c. perpanjangan masa berlaku sertifikat elektronik,
d. pemblokiran dan pencabutan sertifikat elektronik,
e. validasi sertifikat elektronik,

[125] Carlisle Adams dan Steve Lyoyd. *Understanding Public Key Infrastructure*. USA: Macmillan Technical Publishing., 1999.

[126] Informasi sebagaimana dimaksud dalam pasal ini adalah informasi yang minimum harus dipenuhi oleh setiap penyelenggara tanda tangan elektronik.

f. pembuatan daftar sertifikat elektronik yang aktif dan yang dibekukan; dan
g. perjanjian penggunaan sistem dalam Bahasa Indonesia dan bersedia menundukkan diri dalam hukum Indonesia."

Penyelenggara sertifikat elektronik disebut juga dengan CA ini berkedudukan sebagai pihak ketiga yang dipercaya untuk memberikan kepastian atau pengesahan terhadap identitas dari seseorang atau pelanggan (klien atau konsumen yang bersangkutan). Selain itu CA juga mengesahkan pasangan kunci publik dan kunci privat milik orang tersebut sebagaimana yang dimaksud pada Pasal 13 ayat 2 UU ITE yang berbunyi : "Penyelenggara sertifikasi elektronik harus memastikan keterkaitan suatu tanda tangan elektronik dengan pemiliknya."

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 sehingga kekuatan pembuktian yang diperoleh dari informasi dan/atau dokumen elektronik yang telah disertifikasi menjadi lebih kuat ketimbang yang tidak menggunakan sertifikat elektronik.

Selain sebagai bukti otentik, sertifikat keandalan di dalam Pasal 68 RPP menjelaskan bahwa sertifikat keandalan yang dikeluarkan lembaga sertifikasi keandalan bertujuan untuk melindungi konsumen dalam bertransaksi elektronik. Sertifikat keandalan ini merupakan jaminan bahwa pelaku usaha telah memenuhi kriteria yang ditentukan oleh lembaga sertifikasi keandalan sehingga dapat memperkecil pelaku usaha nakal dalam beroperasi. Hal ini dikarenakan kriteria yang diperlukan pelaku usaha dalam memenuhi kriteria ditentukan lembaga sertifikasi keandalan dinilai cukup tinggi sehingga pelaku usaha yang telah memiliki *track record* yang baik yang akan disertifikasi.

Tanggung jawab hukum penyelenggara sertifikat elektronik juga meliputi, sebagai berikut:

1. Tanggung jawab secara perdata

   Adapun tanggung jawab terhadap perdata dalam hal ini merupakan tanggung jawab hukum terhadap adanya perbuatan melawan hukum. Tanggung jawab yang lahir tidak hanya berakibat dari perbuatannya sendiri, melainkan akibat dari perbuatan orang atau benda yang berada di bawah kekuasaannya.[127] Hal ini terdapat di dalam Pasal 1367 KUHPerdata yang berbunyi: "seseorang tidak hanya bertanggung jawab atas kerugian yang disebutkan perbuatannya sendiri, melainkan juga atas kerugian yang disebabkan oleh perbuatan orang-orang yang menjadi tanggungannya, atau disebabkan barang-barang yang berada di bawah pengawasannya."

2. Tanggung jawab secara administratif

   Tanggung jawab yang dimaksud disini lahir dari bentuk pengawasan pihak yang berwenang. Dalam hal ini, penyelenggara sertifikat elektronik dalam menjalankan tugas dan peranannya sebagai pihak yang mengeluarkan sertifikat elektronik diawasi oleh pihak yang berwenang, yaitu pemerintah. Terkait dengan kewenangannya dalam hal tersebut, keberadaan AAUPB (Asas-Asas Umum Pemerintahan yang Baik) merupakan prinsip ataupun norma hukum positif yang telah ada. Sebagai salah satu contoh adalah penerapan asas transparansi. Kelalaian administrator negara terhadap hal tersebut tidak secara tegas dinyatakan sebagai hal yang akan berdampak secara materiil terhadap tindakan ataupun putusan administrator negara.[128]

3. Tanggung jawab pidana

   Tanggung jawab yang diterima dapat berupa teguran tertulis, denda administratif, pemberhentian sementara dan dikeluarkan oleh daftar yang dibuat oleh menteri.[129]

[127] Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik, Op.Cit.*,Hlm. 165.

[128] *Ibid.*, Hlm.159.

[129] RPP Pasal 83 ayat 2.

3.2. Tanggung Jawab Pelaku Usaha Terhadap Konsumen

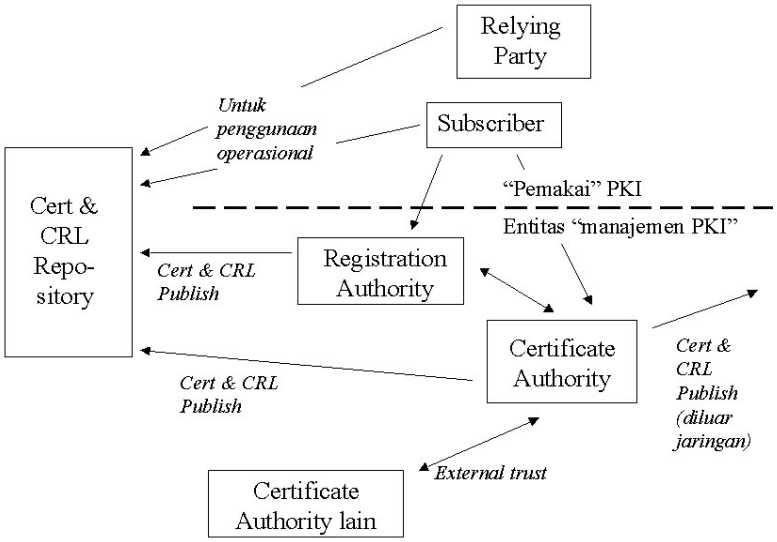
Secara nasional, pranata untuk memberikan perlindungan terhadap konsumen adalah UU No. 8 Tahun 1999 tentang Perlindungan Konsumen (selanjutnya akan disebut dengan UU PK), namun UU PK ini secara khusus belum mengantisipasi perkembangan teknologi informasi di dalam pengaturannya. Dalam penggunaan *Digital Signature* yang telah dijabarkan di bab sebelumnya, kita mengenal adanya dua pihak, yaitu:

1. Certificate Authority (CA),

2. Subscriber,

3. Relying Party.

Hubungan ini menunjukkan kaitan antara CA sebagai penyelenggara jasa atau akan disebut di dalam subbab ini sebagai pelaku usaha sesuai dengan penyebutan di dalam UU PK dan *subscriber* sebagai konsumen. Berdasarkan asumsi tersebut, maka baik hak maupun kewajiban yang ditanggung oleh CA merupakan hak dan kewajiban yang ditanggung oleh pelaku usaha, begitu juga terhadap hak dan kewajiban *subscriber* sama dengan hak dan kewajiban konsumen. Sedangkan *relying party* atau pihak ketiga atau pihak lain yang berkepentingan dalam hal ini adalah para pihak yang secara langsung menghubungkan dirinya dengan *subscriber* dari sebuah CA. Hubungan yang terjadi dapat berupa hubungan transaksi antara pihak yang berkepentingan dengan *subscriber.*



Gambar 4. Entitas dalam infrastruktur kunci publik[130]

Dengan mencermati hubungan hukum para pihak yang berkontribusi dalam penyelenggaraan suatu sistem elektronik, maka paling tidak tanggung jawab hukum penyelenggara sertifikat elektronik meliputi:[131]

1. Tanggung jawab secara pidana kepada setiap pihak terhadap setiap perbuatan peyalahgunaan yang diancam berdasarkan ketentuan pidana (contoh: pemalsuan surat, kesaksian palsu, akses ilegal, intersepsi ilegal, interfensi data dan atau sistem, pemalsuan data, penyalahgunaan perangkat, distribusi konten ilegal dan sebagainya).
2. Tanggung jawab administratif dari setiap instansi untuk memberikan aturan sesuai kewenangan yang dimilikinya, pelanggaran terhadap hal ini administrasi negara yang terkait akan bertanggungjawab terhadap tindakan pembiaran yang merugikan publik. Kemungkinan besar hal tersebut akan mengalir sebagai *class action* dari para konsumen yang dirugikan.
3. Tanggung jawab perdata yang bisa lahir karena UU atau lahir karena hubungan kontraktual para pihak.

[130] http://itasa-ok.blogspot.com/2010/05/public-key-infrastructure_13.html, Public Key Infrastructure, Diposkan oleh Sri Raharjo Saptono P di 09:47 . 13 Mei 2010

[131] Edmon Makarim, *Notaris dan Tanda Tangan Elektronik*, Hlm.128.

Pada dasarnya tanggung jawab perdata akan merujuk pada konsep dan penerapan perbuatan melawan hukum yang dapat ditentukan dalam empat elemen, yaitu:[132]

4. Adanya perbuatan yang bersifat melawan hukum,
5. Adanya kesalahan pelaku (baik karena disengaja maupun lalai) dalam menjalankan kewajiban kehati-hatian,
6. Perbuatan tersebut telah merugikan para pihak lain, dan
7. Adanya hubungan kausalitas antar kerugian dengan perbuatan tersebut.

Sehubungan dengan itu perlu diperhatikan bahwa UNCITRAL *Model Law on e-signature*, memberikan pedoman adanya aturan dalam UU tentang kewajiban dari setiap pihak pengguna TTE, penerima TTE dan penyelenggara TTE itu sendiri.

Perbandingan Tanggung Jawab Para Pihak dalam *E-signature*

Conduct of Signatory	**Conduct of the CSP**	**Conduct of Relying Party**
Article 8 *Conduct of the signatory* 1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall: (a) Exercise reasonable care to avoid unauthorized use of its signature creation data; (b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if: (i) The signatory knows that the signature creation data have been compromised; or (ii) The circumstances	*Article 9* *Conduct of the certification service provider* 1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall: (a) Act in accordance with representations made by it with respect to its policies and practices; (b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate; (c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate: (i) The identity of the certification service provider; (ii) That the signatory that is identified in the certificate had control of the signature creation data at the time	*Article 11* *Conduct of relying party* A relying party shall bear the legal consequences of its failure: (a) To take reasonable steps to verify the reliability of an electronic signature; or (b) Where an electronic signature is supported by a certificate, to take reasonable steps: (i) To verify the validity, suspension or revocation of the certificate; and (ii) To observe any limitation with respect to the certificate.

[132] *Ibid.*, Hlm. 128.

known to the signatory give rise to a substantial risk that the signature creation data may have been compromised; (c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate. 2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.	when the certificate was issued; (iii) That signature creation data were valid at or before the time when the certificate was issued; (d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise: (i) The method used to identify the signatory; (ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used; (iii) That the signature creation data are valid and have not been compromised; (iv) Any limitation on the scope or extent of liability stipulated by the certification service provider; (v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law; (vi) Whether a timely revocation service is offered; (e) Where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service; (f) Utilize trustworthy systems, procedures and human resources in performing its services. 2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.	

Tabel 2. Perbandingan Tanggung Jawab Para Pihak dalam *E-signature*[133]

Tanggung jawab CA terhadap konsumennya sangat berpengaruh terhadap tingkat *trustworthy* dari CA itu sendiri karena apabila suatu CA menjalankan usahanya secara bertanggung jawab, dalam hal ini berarti

[133] *Ibid.*, Hlm. 130-131.

berdasarkan prinsip kehati-hatian dan berdasarkan standar secara maksimal, hasil atau *output* yang keluar dari proses usahanya tersebut juga akan bagus sesuai dengan proses yang dijalankannya.[134] Berdasarkan dengan penjelasan di atas, maka CA sebagai pelaku usaha harus selalu waspada dalam menjalankan usahanya sehingga tidak mengabaikan kepentingan konsumen.

3.2.1. Tanggung Jawab Pelaku Usaha dalam menjamin hak konsumen

Sebagai penyelenggara jasa atau pelaku usaha, CA harus menjamin hak-hak *subscriber* antara lain:

1. *Privacy*

   Dalam pasal 4 butir 1 UU PK menyatakan bahwa konsumen berhak atas kenyamanan, keamanan dan keselamatan dalam mengkonsumsi barang dan/atau jasa. Contoh: Ketika *subscriber* meng"*apply*" kepada CA, *subscriber* akan dimintai keterangan mengenai identitasnya, besar kecilnya keakuratan dari identitas tersebut tergantung dari jenis tingkatan sertifikat tersebut. Semakin tinggi tingkat sertifikat maka semakin akurat pula identitas sebenarnya dari *subscriber*.

   Namun dalam hal ini yang perlu diperhatikan adalah CA sebagai penyimpan data berkewajiban menjaga kerahasiaan identitas *subscriber* dari pihak yang tidak berkepentingan. CA hanya boleh meng-c*onfirm* bahwa sertifikat yang dimiliki oleh *subscriber* adalah benar dan diakui oleh CA.

   Di beberapa negara maju, data pribadi mendapat perlindungan dalam undang-undang (*data protection act*). Di dalam undang-undang yang bersangkutan tercantum prinsip perlindungan data (*Data Protection Principles*) yang harus ditaati oleh orang-orang yang menyimpan atau memproses informasi dengan mempergunakan komputer via internet yang menyangkut kepentingan orang banyak. Biro-biro komputer yang menyediakan jasa pelayanan bagi mereka

[134] Edmon Makarim. *Hukum telematika, Op.Cit.,* hlm.408.

yang hendak memproses informasi juga harus dikontrol dan harus melakukan pendaftaran menurut undang-undang tersebut. Konsumen yang informasi dirinya disimpan pada komputer diberi hak-hak untuk mengakses dan hak untuk memperoleh catatan-catatan pembetulan dan penghapusan informasi yang tidak benar. Mereka pun dapat mengajukan pengaduan kepada *Data Protection Registar* (yang diangkat berdasarkan undang-undang) apabila mereka tidak merasa puas terhadap cara orang atau organisasi yang mengumpulkan informasi dan dalam keadaan-keadaan tertentu konsumen memiliki hak atas ganti kerugian.

Pelanggaran terhadap prinsip-prinsip perlindungan data dapat menyebabkan tanggung jawab pidana, adapun prinsip-prinsip tersebut antara lain:

1. Informasi yang dimuat dalam data pribadi harus diperoleh dan data pribadi itu harus diproses, secara jujur dan sah.
2. Data pribadi harus dipegang hanya untuk satu tujuan atau lebih yang spesifik dan sah.
3. Data pribadi yang dikuasai untuk satu tujuan dan tujuan-tujuan tidak boleh digunakan atau disebarluaskan dengan melalui suatu cara yang tidak sesuai dengan tujuan-tujuan tersebut.
4. Data pribadi yang dikuasai untuk keperluan suatu tujuan harus layak, relevan dan tidak terlalu luas dalam,
5. Data pribadi harus akurat dan selalu *up-to date.*
6. Data pribadi yang dikuasai untuk keperluan suatu tujuan tertentu tidak boleh dikuasai terlalu lama dari waktu yang diperlukan untuk kepentingan tujuan tersebut.
7. Tindakan-tindakan pengamanan yang memadai harus diambil untuk menghadapi akses secara tidak sah atau pengubahan, penyebarluasan atau perusakkan data pribadi serta menghadapi kerugian tidak terduga.

8. Seorang individu akan diberikan hak untuk:
   a. Dalam jangka waktu yang wajar dan tanpa kelambatan serta tanpa biaya, yaitu dengan diberi penjelasan oleh pihak pengguna data tentang apakah pihaknya menguasai data pribadi di mana individu yang bersangkutan menjadi subyek data. Dan untuk akses pada suatu data demikian yang dikuasai oleh pihak pengguna data.
   b. Jika dipandang perlu, melakukan perbaikan atau penghapusan data.

Prinsip yang terakhir berkaitan dengan pengamanan dan ancaman terhadap hal ini ada dua jenis:

1. Pengamanan dari akses tidak sah, dan
2. Berkaitan dengan *copy-copy back up* pusat-pusat data yang berisi data pribadi.

Masih berkaitan dengan masalah jaminan *privacy* dalam kaitannya dengan kunci privat adalah harus adanya jaminan bahwa CA tidak berusaha mencari pasangan kunci publik dari *subscriber*. CA mempunyai peluang yang besar untuk bisa menemukan kunci pasangan dari *subscriber* karena CA mempunyai komputer yang lebih canggih untuk menemukannya.

Selain itu harus ada jaminan bahwa pencipta kartu yang berisikan kunci privat juga tidak akan menyebarluaskan ataupun menggandakannya. Hal ini sangat logis sekali karena pembuat kartu selain mengetahui kunci publik juga mengetahui kunci privatnya karena ia adalah penciptanya. Untuk menjamin hal ini perlu adanya suatu *notary system* yang menjamin hal tersebut.

2. *Accuracy*

Termaktub dalam pasal 4 butir 2, 3 dan 8 UU PK[135]. Dalam prinsip ini terkandung pengertian ketepatan antara apa yang diminta dengan apa yang didapatkan. Bahwa apa yang didapat oleh *subscriber* sesuai dengan apa yang ia minta berdasarkan informasi yang diterimanya. Ketepatan informasi (informasi yang benar tanpa tipuan) juga merupakan prinsip *accuracy*. Sebagai contoh: *subscriber* yang meminta level tertentu dari sertifikat sebaiknya tidak diberikan level yang lebih rendah atau lebih tinggi.

CA juga berkewajiban memberitahukan segala keterangan yang berkaitan dengan penawaran maupun permintaan yang diajukan. Secara tidak langsung *subscriber* berhak untuk mendapatkan CA yang berlisensi artinya ketika *subscriber* mengakses ke CA, terdapat praduga bahwa CA adalah CA yang sah dan berlisensi dan *subscriber* harus dilindungi dari penyimpangan CA yang tidak benar atau gadungan.

3. *Property*

Pasal 4 butir 8 UU PK yang menyatakan bahwa konsumen berhak untuk mendapatkan kompensasi, ganti rugi dan/atau penggantian, apabila barang dan/atau jasa yang diterima tidak sesuai dengan perjanjian atau tidak sebagaimana mestinya. *Subscriber* harus dilindungi hak miliknya dari segala penyimpangan yang mungkin terjadi akibat masuknya *subscriber* ke dalam sistem ini. Artinya *subscriber* berhak dilindungi dari segala bentuk penyadapan, penggandaan, pencurian serta bentuk-bentuk penyalahgunaan yang

[135] Pasal 4 butir 2 berbunyi : "Hak konsumen adalah hak untuk memilih barang dan/atau jasa serta mendapatkan barang dan/atau jasa tersebut sesuai dengan nilai tukar dan kondisi serta jaminan yang dijanjikan."

Pasal 4 butir 3 berbunyi: "Hak konsumen adalah hak atas informasi yang benar, jelas dan jujur mengenai kondisi dan jaminan barang dan/atau jasa yang digunakan."

Pasal 8 mengatur tentang perbuatan yang dilarang bagi pelaku usaha dalam memproduksi dan/atau memperdagangkan, dilarang menawarkan barang dan/atau jasa secara tidak benar, dilarang menyesatkan konsumen, dilarang menggunakan ancaman serta pemaksaan terhadap konsumen dan perbuatan-perbuatan lainnya yang dapat merugikan konsumen.

dapat mengakibatkan kerugian padanya. Jika hal ini terjadi, maka CA berkewajiban mengganti kerugian yang diderita oleh *subscriber*.

4. *Accessibility*

   Termaktub dalam pasal 4 butir 4, 5, 6 dan 7 UU PK[136]. Bahwa setiap pribadi berhak medapat perlakuan yang sama dalam hal untuk mengakses dan informasi. Artinya tiap *subscriber* bisa masuk ke dalam sistem ini jika memenuhi persyaratan dan ia bisa mempergunakan sistem ini tanpa adanya hambatan. *Subscriber* juga berhak untuk didengar pendapat dan keluhannya.

Hak-hak konsumen untuk tercapainya perlindungan konsumen sudah tercantum atau dituangkan dalam UU PK. Hal ini dapat diartikan bahwa hak-hak tersebut telah diakui keberadaannya dan memiliki kepastian hukum. Upaya hukum yang dilakukan oleh konsumen yang merasa dirugikan dapat menggunakan pasal-pasal dalam UU PK. Dalam kaitannya dengan penggunaan *digital signature*, CA dalam kedudukan yang lebih kuat harus bisa menjamin hak-hak konsumen. Terutama dalam perjanjian adhesi antara CA dan *subscriber*.

Perjanjian diajukan sebaiknya tidak hanya berat sebelah sehingga *subscriber* tetap mempunyai posisi penawaran (*bargaining power*). Untuk memperkecil segala macam resiko, CA dapat mengasuransikan resiko tersebut. Hal ini untuk mengurangi beban yang harus ditanggung oleh CA apabila suatu saat ada konsumen (*subscriber*) yang menuntut CA karena merasa dirugikan. Namun, tetap harus ada upaya sebaik mungkin dengan itikad baik dari kedua belah pihak serta menjalankan

[136] Pasal 4 butir 4 berbunyi: "hak konsumen adalah hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan."

Pasal 4 butir 5 berbunyi: " hak konsumen adalah hak untuk mendapatkan advokasi, perlindungan dan upaya penyelesaian sengketa perlindungan konsumen secara patut."

Pasal 4 butir 6 berbunyi: "hak konsumen adalah hak untuk mendapat pembinaan dan pendidikan konsumen."

Pasal 4 butir 7 berbunyi" "hak konsumen adalah hak untuk diperlakukan atau dilayani secara benar dan jujur serta tidak diskriminatif." Hak untuk diperlakukan atau dilayani secara benar dan jujur serta tidak diskriminatif berdasarkan suku, agama, budaya, daerah, pendidikan, kaya, miskin, dan status sosial lainnya.

prinsip kehati-hatian merupakan bentuk awal pencegahan resiko-resiko yang ada di kemudian hari.

3.2.2. Tanggung Jawab Pelaku Usaha dalam Melindungi Konsumen

Selain hak konsumen, dalam UU PK diatur pula hak dan kewajiban pelaku usaha serta larangan-larangan yang bertujuan untuk memberi perlindungan terhadap konsumen. Adapun kewajiban pelaku usaha tertuang dalam Pasal 7 UU PK[137]. Selain tanggung jawab kepada konsumen, penyelenggara juga bertanggung jawab untuk mengikuti standar yang lazim berlaku dalam komunitasnya dan/atau terhadap penerapan pedoman pemerintah sebagai patokan melakukan upaya yang terbaik dan menjaga mutu penyelenggaraan jasanya (*Quality of Secrvice*).[138]

3.2.3. Tanggung Jawab Pelaku Usaha dalam hal Ganti Rugi

Dalam UU PK diatur pula tanggung jawab pelaku usaha yang tertuang di dalam Bab VI mengenai tanggung jawab pelaku usaha, dimana diatur di dalam pasal 19 sampai pasal 28. Tanggung jawab pelaku usaha di dalam UU PK dapat disimpulkan sebagai berikut:

1. Tanggung jawab dalam memberikan ganti rugi atas kerusakan, pencemaran, dan/atau kerugian konsumen akibat mengkonsumsi barang dan/atau jasa yang dihasilkan atau diperdagangkan (Pasal 19 ayat 1 UU PK),
2. Tanggung jawab atas iklan yang diproduksi dan segala akibat yang ditimbulkan oleh iklan tersebut (Pasal 20 UU PK),

---

[137] Pasal 7 UU PK berbunyi : "Kewajiban pelaku usaha adalah :
a. beritikad baik dalam melakukan kegiatan usahanya;
b. memberikan informasi yang benar, jelas dan jujur mengenai kondisi dan jaminan barang dan/atau jasa serta memberi penjelasan penggunaan, perbaikan dan pemeliharaan;
c. memperlakukan atau melayani konsumen secara benar dan jujur serta tidak diskriminatif;
d. menjamin mutu barang dan/atau jasa yang diproduksi dan/atau diperdagangkan berdasarkan ketentuan standar mutu barang dan/atau jasa yang berlaku;

[138] Edmon Makarim. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik.* Jakarta: PR Rajagrafindo Persada. 2010. Hlm.319.

3. Tanggung jawab sebagai importir barang dan/atau jasa (Pasal 21 ayat 1 dan 2 UU PK),
4. Tanggung jawab atas tuntutan ganti rugi dan/atau gugatan konsumen apabila:
   a. Pelaku usaha lain menjual kepada konsumen tanpa melakukan perubahan apa pun atas barang dan/atau jasa tersebut;
   b. Pelaku usaha lain di dalam transaksi jual beli tidak mengetahui adanya perubahan barang dan/atau jasa yang dilakukan oleh pelaku usaha atau tidak sesuai dengan contoh, mutu dan komposisi. (Pasal 24 Ayat 1 UU PK)
5. Tanggung jawab dalam memenuhi jaminan atau garansi sesuai dengan yang diperjanjikan. (Pasal 25 ayat 1 dan 26 UU PK).

3.2.4. Pengecualian Pelaku Usaha dalam Tanggung Jawabnya

Adapula pengecualian pelaku usaha dalam tanggung jawab atas kerugian yang diderita konsumen. Hal ini tertuang di dalam Pasal 27 UU PK yang menyatakan bahwa pelaku usaha yang memproduksi barang dibebaskan dari tanggung jawab atas kerugian yang diderita konsumen, apabila:

a. Barang tersebut terbukti seharusnya tidak diedarkan atau tidak dimaksudkan untuk diedarkan;
b. Cacat barang timbul pada kemudian hari (cacat timbul di kemudian hari adalah sesudah tanggal mendapat jaminan dari pelaku usaha sebagaimana diperjanjikan, baik tertulis maupun lisan);
c. Cacat timbul akibat ditaatinya ketentuan mengenai kualifikasi barang (yang dimaksud dengan kualifikasi barang adalah ketentuan standarisasi yang telah ditetapkan pemerintah berdasarkan kesepakatan semua pihak);
d. Kelalaian yang diakibatkan oleh konsumen;

e. Lewatnya jangka waktu penuntutan 4 (empat) tahun sejak barang dibeli atau lewatnya jangka waktu yang diperjanjikan (waktu yang diperjanjikan adalah masa garansi).

Dalam hal pelaku usaha terbebas dari tanggung jawab sebagaimana yang dimaksud pasal 27 UU PK, beban pembuktian terhadap ada tidaknya unsur kesalahan dalam gugatan ganti rugi merupakan tanggung jawab pelaku usaha. Pelaku usaha yang wajib membuktikan dalam hal ini.

Seperti yang telah dijelaskan pada subbab sebelumnya, di dalam Pasal 15 UU ITE, pelaku usaha bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya dan bertanggung jawab penuh terhadap penyelenggaraan sistem elektronik itu sendiri, kecuali jika dapat dibuktikan adanya keadaan memaksa, kesalahan dan/atau kelalaian yang diakibatkan oleh pihak pengguna, dalam hal ini konsumen atau *subscriber*.

Namun, perlindungan hak konsumen dalam transaksi elektronik masih sangatlah rentan. Walaupun UU PK dan UU ITE telah mengatur hak dan kewajiban bagi pelaku usaha dan konsumen, namun kurang tepat untuk diterapkan dalam transaksi elektronik. Kemajuan ilmu pengetahuan dan teknologi dalam proses produksi barang dan jasa ternyata belum diikuti dengan kemajuan perangkat hukum yang ada.

3.3. Analisis Tanggung Jawab Hukum Kasus DigiNotar

Dalam prakteknya sekarang ini, notaris sebenarnya tidak hanya memiliki peran dan kewenangan dalam transaksi yang konvensional, khususnya dalam pembuatan akta otentik saja, melainkan juga pekerjaan lain sebagaimana ditentukan oleh peraturan perundang-undangan. Bahkan dalam lingkup IT di Belanda, Notaris dapat menjadi pihak ketiga terpercaya dalam suatu transaksi elektronik atau menjadi *escore* untuk *source-code software* komputer.

Dalam lingkup transaksi yang tidak hanya konvensional melainkan juga secara elektronik, notaris dapat berperan penting dalam mencegah penipuan (*Fraud*). Perkembangan notaris konvensional menjadi notaris modern bukan hanya dinilai berdasarkan adanya penggunaan komputerisasi dan internet pada administrasi kantor notaris saja, melainkan juga lebih ditandai dengan meningkatnya fungsi dan peran notaris dalam suatu transaksi elektronik atau bahkan menyelenggarakan jasanya secara elektronik. Dalam perkembangannya fungsi dan peran tersebut dipopulerkan dengan istilah *Cybernotary* dan/atau *Electronic Notary*.[139]

Semula memang berdasarkan konsep ABA (*American Bar Association, Information Security Committee*) yang mempopulerkan istilah *cybernotary* sebenarnya merujuk kepada fungsi dan peran CA/CSP yang dianggapnya sebagaimana layaknya notaris dalam *Cyberspace,* oleh karena itu mereka menyebutnya sebagai *cybernotary*. Sementara *electronic notary* yang diusung oleh TEDIS adalah pekerjaan profesi hukum untuk melakukan dukungan kegiatan notarisasi secara elektronik.[140]

Di Belanda, spesialisasi notaris terkait TI berbentuk dua hal, yakni:

1. Sebagai T3P, dan
2. Menjalankan fungsi *escrow-agreement* terhadap *source code* program komputer.[141]

Salah satu bentuk nyata bahwa notaris menjadi pihak ketiga adalah dengan adanya DigiNotar sebagai lembaga yang menawarkan layanan, dalam hal ini merupakan produk hukum resmi terkait dengan notaris. DigiNotar awalnya dibentuk pada tahun 1997 oleh notaris Belanda, Dick Batenburg dari *Beverwijk* dan *Koninklijke Beroepsorganisatie Notariele,* badan nasional untuk notaris hukum sipil Belanda. KNB menawarkan semua jenis layanan notaris ke pusat dan dikarenakan begitu banyaknya layanan yang ditawarkan adalah prosedur hukum resmi terkait dengan notaris, maka keamanan dalam komunikasi menjadi peran yang penting. KNB menawarkan layanan konsultasi

[139] Edmon Makarim, *Notaris dan Tanda Tangan Elektronik. Op.Cit.*, hlm.84.
[140] *Ibid.*
[141] *Ibid.*

kepada anggotanya tentang bagaimana menerapkan layanan elektronik dalam bisnis mereka, salah satunya kegiatan yang menawarkan sertifikat yang aman.

Dick Batenburg dan KNB membentuk kelompok TTP (*Trusted Third Party*) *Notarissen* (TTP Notaris). TTP merupakan pihak ketiga terpercaya. Seorang notaris dapat menjadi anggota TTP-*Notarissen* jika mereka mematuhi aturan-aturan tertentu. Jika mereka mematuhi aturan tambahan tentang prosedur pelatihan dan pekerjaan, mereka dapat menjadi TTP notaris yang terakreditasi.

DigiNotar adalah otoritas sertifikat Belanda yang dimiliki oleh Vasco Data Security International. Pada tanggal 3 September 2011, setelah menjadi jelas bahwa pelanggaran keamanan telah mengakibatkan penipuan penerbitan sertifikat, pemerintah Belanda mengambil alih manajemen operasional sistem DigiNotar. Pada bulan yang sama, perusahaan ini pun dinyatakan bangkrut.

Kegiatan utama DigiNotar sebagai Otoritas Sertifikat mengeluarkan dua jenis sertifikat. Pertama, mereka mengeluarkan sertifikat dengan nama mereka sendiri (di mana *root* CA bernama "DigiNotar *Root* CA"). Sertifikat ini tidak dikeluarkan lagi sejak Juli 2010 walau ada beberapa masih berlaku sampai dengan Juli 2013. Kedua, mereka mengeluarkan sertifikat untuk pemerintah Belanda *PKIoverheid* ("*PKIgovernment*") program. Penerbitan ini adalah melalui dua sertifikat menengah, masing-masing yang dirantai sampai dengan satu dari dua "*der Nederlanden Staat*" *root* CA. Pemerintah Belanda, pemerintah lokal dan organisasi menawarkan layanan bagi pemerintah yang ingin menggunakan sertifikat untuk komunikasi internet yang aman. Beberapa layanan elektronik yang paling ditawarkan dan digunakan oleh pemerintah Belanda adalah sertifikat dari DigiNotar. Contohnya adalah otentikasi infrastruktur DigiNotar dan *auto-registration center Rijksdienst voor het Wegverkeer organization*.

Sebelum kita membahas kasus yang menimpa DigiNotar dan konsekuensi buruk di baliknya, ada baiknya jika kita memahami dulu sistem kerja dari protokol HTTPS alias HTTP *Secure*. Protokol ini merupakan gabungan dari protokol HTTP dengan SSL/TLS yang bertujuan memberi keamanan ekstra bagi pengguna internet.

Pada HTTP biasa, lalu lintas data dari server di internet dengan komputer pengguna berjalan polos tanpa perlindungan apapun. Metode ini jamak dilakukan untuk mengakses situs standar, seperti *Kompas.com* atau *InfoKomputer.com*. Dalam situs standar ini hanya berita yang bukan rahasia dan boleh disebarluaskan sehingga apabila informasi tersebut diubah oleh orang yang tidak bertanggung jawab dampaknya hanya pada lingkungan kecil saja. Namun metode HTTP menjadi tidak sesuai apabila digunakan untuk mengakses *Gmail, Facebook*, dan semua layanan yang membutuhkan *username* dan *password*. Hal ini dikarenakan apabila kita mengirim *username* dan *password* ke server-server tersebut, oknum yang tidak bertanggungjawab dapat mencegat data yang dikirim dan memperoleh *username* dan *password* kita. Mengingat pentingnya data tersebut, maka situs yang membutuhkan *ussername* dan *Password* seperti ini menggunakan protokol HTTPS.

Pada protokol HTTPS, seluruh lalu lintas data dienkripsi alias diacak dengan kunci yang diberikan situs layanan tersebut. Ketika mengakses *https://www.facebook.com*, selain menerima halaman utama Facebook sebenarnya yang diterima merupakan sebuah *public key* yang dikirim oleh Facebook. Ketika kita memasukkan *username* dan *password*, data tersebut langsung dienkripsi menggunakan *public key* tersebut. Pembuka kunci enkripsi itu hanya dimiliki *Facebook* sehingga hanya mereka yang bisa membukanya sehingga data tersebut lebih aman dan sulit dibaca oleh orang yang tidak bertanggungjawab. Meski protokol HTTPS lebih aman tetapi tidak luput dari penyalahgunaan. Dua metode penyalahgunaan yang sering dilakukan adalah *phishing* dan *Man-in-the-middle* (MITM). Pada kedua metode tersebut, *hacker* alias orang yang berniat jahat bisa membuat situs tiruan yang nyaris sama dengan situs asli, termasuk membuatnya dengan protokol HTTPS.

Ketika calon mangsa terjebak dan masuk ke situs palsu tersebut, sang *hacker* tetap akan mengirimkan *public key* dan halaman yang persis seperti situs aslinya. Hal yang membedakan hanya kunci pembuka *public key* tersebut dimiliki oleh sang *hacker*. Dengan demikian, enkripsi HTTPS tidak berguna lagi dan sang *hacker* tetap bisa mendapatkan *username* dan *password* Anda.

Hal inilah yang menyebabkan protokol HTTPS perlu mendapat pengamanan lebih dari *browser* melalui sistem sertifikat digital. Apabila *browser* mengeluarkan peringatan kurang lebih menyebutkan kalau *browser* tidak menemukan sertifikat yang valid atau sertifikat yang ada tidak dipercaya oleh browser, maka hal yang terbaik adalah keluar dari situs tersebut.

Lembaga yang dapat mengeluarkan sertifikat digital ini sendiri disebut *Certificate Authority* (CA). Seperti yang telah dijabarkan di bab sebelumnya, CA akan memberikan *public key* yang dapat digunakan situs bersangkutan kepada setiap orang yang mengaksesnya. Ada ratusan lembaga CA di dunia, beberapa yang terkenal adalah adalah *VeriSign, GoDaddy,* dan *Comodo*. Setiap *browser* sudah dilengkapi daftar CA yang terpercaya, yang merupakan hasil audit lembaga independen *WebTrust*. Jadi, tidak semua lembaga CA masuk ke daftar terpercaya *browser*.

Lembaga CA sendiri sangat berhati-hati memberi sertifikat CA kepada sebuah situs. Mereka akan mengecek latar belakang perusahaan, orang yang bertanggung jawab terhadap *security* situs tersebut, bahkan terkadang melakukan konfirmasi silang ke lembaga pemerintahan yang bersangkutan. Harga sebuah sertifikat juga tidak murah, yaitu sekitar US$400-1500 untuk produk-produk *VeriSign*. Hal ini mengakibatkan banyak situs internal perusahaan tidak memiliki sertifikat digital. Namun untuk situs publik (apalagi perbankan), diwajibkan memiliki sertifikat digital.

Kasus yang menimpa DigiNotar menimbulkan pertanyaan besar soal keefektifan sertifikat digital, dimana DigiNotar merupakan salah satu perusahaan penjual sertifikat keamanan SSL yang digunakan untuk memastikan keaslian situs dan menjamin keamanan laju komunikasi antara pengguna dan situs tersebut. Pada tanggal 10 Juli 2011, sebuah *wildcard* sertifikat dikeluarkan oleh sistem DigiNotar untuk *Google* oleh seorang penyerang dengan akses ke sistem mereka. Sertifikat ini kemudian digunakan oleh orang tak dikenal di Iran untuk melakukan serangan *man-in-the-middle* terhadap layanan *Google*. Pada tanggal 28 Agustus 2011, masalah sertifikat yang diamati pada beberapa penyedia layanan Internet di Iran. Menurut siaran berita berikutnya oleh Vasco,

DigiNotar telah mendeteksi adanya penyusupan ke dalam infrastruktur kewenangan sertifikatnya pada tanggal 19 Juli 2011. DigiNotar tidak secara terbuka mengungkapkan adanya pelanggaran keamanan.

Setelah sertifikat ini ditemukan, DigiNotar terlambat mengakui puluhan sertifikat palsu telah dibuat, termasuk sertifikat untuk domain dari *Yahoo!, Mozilla, Wordpress* dan Proyek Tor. DigiNotar tidak dapat menjamin semua sertifikat tersebut telah dicabut. Investigasi oleh *F-Secure* juga mengungkapkan bahwa *website* DigiNotar itu telah dirusak oleh *hacker* Iran pada 2009. Seorang *hacker* asal Iran dengan *nickname "Comodohacker"* ini dapat masuk ke dalam *database* DigiNotar dan mencuri sertifikat digital. Sertifikat digital yang dicuri berjumlah 531 buah yang digunakan *Google, Facebook, Skype, Mozilla, Twitter,* bahkan lembaga keamanan CIA dan Mossad.

Menurut para ahli, *hacker* telah berhasil membuat 532 setifikat palsu di 344 domain. Di antaranya adalah *Google, Yahoo, Facebook, Microsoft, Skype, AOL, Mozilla, TorProject* dan *WordPress.* Situs mata-mata seperti CIA, *Mossad* dan MI6 juga berhasil dipalsukan sertifikatnya. Kasus peretasan Diginotar ini menyebabkan lebih dari 300,000 *email* akun *Gmail* milik warga negara Iran bocor (karena kebetulan Iran tidak memiliki CA sendiri dan mengandalkan DigiNotar sebagai CA).

Di lain pihak, DigiNotar patuh terhadap semua ketentuan teknis keamanan di atas kertas dan juga lulus semua proses audit. Namun berdasarkan penyelidikan Fox-IT yang mengaudit kebobolan DigiNotar menemukan fakta mengejutkan yaitu server DigiNotar memiliki sistem keamanan yang lemah, yaitu server tidak ter-*update* dengan baik, tidak ada perlindungan antivirus, serta disusupi banyak *malware*.

Berdasarkan peristiwa tersebut, banyak yang menghapus sertifikat yang dikeluarkan DigiNotar, seperti *Microsoft, Internet Explorer, Apple Safari, Google Chrome,* dan *Mozilla Firefox*. Namun, perlindungan ini terbatas pada domain *Google*, yang mengakibatkan *Google* menghapus DigiNotar dari daftar terpercaya penerbit sertifikat. Pada tanggal 9 September 2011, *Apple* mengeluarkan *Security Update* 2011-005 untuk Mac OS X 10.6.8, 10.7.1 dan

menghilangkan DigiNotar dari daftar sertifikat *root* terpercaya dan otoritas sertifikat EV. Tanpa pembaruan ini, Safari dan Mac OS X tidak mendeteksi pencabutan sertifikat, dan pengguna harus menggunakan *Keychain utilitas* secara manual menghapus sertifikat tersebut.

Pemerintah Belanda mengumumkan pada tanggal 3 September 2011, bahwa mereka akan beralih ke perusahaan yang berbeda sebagai otoritas sertifikat. Pada tanggal 20 September 2011, Vasco mengumumkan bahwa DigiNotar yang merupakan anak perusahaannya dinyatakan bangkrut setelah diputus di pengadilan Haarlem. Pengadilan segera menunjuk seorang wali untuk mengambil alih manajemen dari semua urusan DigiNotar.

Menurut pendapat penulis, DigiNotar sebagai CA seharusnya mengambil langkah cepat setelah mengetahui adanya pembobolan sertifikat yang dikeluarkannya. DigiNotar seharusnya bisa menggunakan kewenangannya dalam memblokir atau mencabut sertifikat elektronik sebagai langkah awal menyingkapi peretasan tersebut. Namun DigiNotar tidak melakukan tindakan tersebut sehingga para pelanggan atau konsumennya yang terlebih dahulu mengambil tindakan, yaitu menarik atau menghapus sertifikat yang dikeluarkan DigiNotar seperti *Microsoft, Internet Explorer, Apple Safari, Google Chrome, Mozilla Firefox* dan lain sebagainya.

Hal yang patut dicermati kembali adalah persoalan sistem keamanan teknologi yang digunakan DigiNotar yang mana diketahui bahwa DigiNotar patuh terhadap semua ketentuan teknis keamanan di atas kertas dan juga lulus semua proses audit, namun ditemukan server DigiNotar memiliki sistem keamanan yang lemah, seperti server yang tidak ter-*update* dengan baik, tidak ada perlindungan antivirus, serta disusupi banyak *malware*. Padahal mengingat DigiNotar merupakan CA yang berperan penting menjaga keamanan dan melindungi data pelanggan atau konsumennya, seharusnya DigiNotar memiliki sistem keamanan yang kuat, ter-*update* dengan baik agar sulit disusupi pertahanannya.

Melihat permasalahan DigiNotar jika dihubungkan dengan tanggung jawab penyelenggara yang terdapat di dalam *Article* 6 EC *Directive* yang berbunyi:

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:
   (a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
   (b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
   (c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;

   unless the certification-service-provider proves that he has not acted negligently.
2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.
3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate. provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.

2. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties.

   The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.

Berdasarkan kasus yang terjadi pada DigiNotar ini, dapat dikatakan bahwa DigiNotar telah lalai dalam menjaga dan melindungi data atau informasi konsumennya dengan tidak mengindahkan praktek kelaziman bisnis yang berkembang dengan upaya yang terbaik atau tidak memperhatikan standar-standar atau pedoman pembinaan penyelenggaraan yang berlaku atau yang telah ditetapkan instansi terkait sehingga mengakibatkan konsumennya dirugikan. Sehingga sudah selayaknya DigiNotar diberlakukan tanggung jawab hukum secara ketat (*strict liability*), dimana tidak perlu lagi dibuktikan oleh penggugat tentang kesalahannya. Mengingat adanya teori keadilan interaktif yang menyatakan bahwa setiap orang diberlakukan konsekuensi hukum terhadap setiap tindakannya, maka sepantasnya diberlakukan pula konsekuensi hukum terhadap tindakan DigiNotar.

Penyelenggara CA pun dituntut untuk dapat menyelenggarakan sistemnya secara handal, aman dan bertanggung jawab (Pasal 15 dan 16 UU ITE), dalam hal ini DigiNotar terbukti tidak menyelenggarakannya secara aman. Selain itu, dengan adanya beberapa faktor (*Trustworthy*) di dalam UNCITRAL *Model Law on Electronic Signatures with Guide to Enactment* 2001 yang telah dijabarkan bab sebelumnya, maka baik sumber daya manusia, kualitas perangkat keras dan sistem perangkat lunak, dan lain sebagainya, membuat DigiNotar tidak memenuhi standar yang telah ditetapkan tersebut.

BAB IV
Kesimpulan dan Saran

4.1. Kesimpulan

Adapun kesimpulan yang dapat ditarik sebagai berikut:

1. Dalam pengaturan hukum mengenai TTE, autentikasi dan verifikasi menjadi fungsi utama. TTE juga memberikan terobosan sebagai salah satu alat bukti baru. Dengan adanya *secured communication* (*Confidentiality, Integrity, Authorization, Availability, Authenticity, Non-Repudiation,* dan *Auditability* /CIAANA) sebagai bentuk minimal yang harus dipenuhi, sehingga diperlukan CA sebagai penyelenggara sertifikat elektronik mengakibatkan TTE semakin sulit dibantah atau disangkal. Begitu pula dengan transaksi yang dibubuhi TTE, dalam hal ini tanda tangan digital yang tersertifikasi dan terakreditasi yang dibubuhi di dalam transaksi elektronik memiliki kekuatan hukum yang sama seperti transaksi konvensional. Selain itu, pengaturan hukum mengenai TTE di Belanda dibaginya menjadi 2, yaitu adanya TTE tersertifikasi dibuat dengan menggunakan jasa penyelenggara sertifikasi elektronik sehingga dapat disebut dengan *advanced electronic signature* (nilai kekuatannya kuat) sedangkan TTE yang tidak tersertifikasi dibuat tanpa menggunakan jasa penyelenggara sertifikasi elektronik, dapat disebut juga dengan *ordinary electronic signature* (nilai kekuatannya kurang kuat).
2. Tanggung jawab hukum penyelenggara TTE mencermati kasus DigiNotar berdasarkan BW dan *e-signature act* di Belanda, maka dapat dibagi sebagai berikut:
    a. Tanggung jawab administratif

       Pemerintah dalam hal ini berperan serta mengambil tindakan untuk mempailitkan DigiNotar yang telah merugikan konsumen dan kepentingan publik. Namun, tidak melakukan peran serta dalam membantu DigiNotar menyelesaikan permasalahannya dengan konsumen DigiNotar tersebut.

b. Tanggung jawab perdata

DigiNotar telah melakukan perbuatan melawan hukum, dalam hal ini terlihat bahwa adanya kebocoran data atau informasi konsumennya. Sehingga hubungan kontraktual antara DigiNotar dan konsumen dimana seharusnya DigiNotar dalam hal ini menjamin keamanan dan melindungi data atau informasi yang telah diberikan kepadanya telah bocor kepada pihak yang tidak bertanggung jawab, sehingga DigiNotar berhak bertanggung jawab karena telah lalai melindungi data atau informasi tersebut.

c. Tanggung jawab pidana

DigiNotar telah diberikan sanksi administratif dengan menganti rugi kerugian yang diderita oleh para konsumennya.

Apabila kasus yang menimpa DigiNotar terjadi pada CA di Indonesia, maka dalam menyikapinya tanggung jawab yang ada dapat dijabarkan sebagai berikut:

a. Tanggung jawab administrasi

Dalam hal ini, seharusnya pemerintah ikut andil dalam menyikapi permasalahan CA yang ada. Hal ini dikarenakan pemerintah memiliki peran sebagai pengawas dan pemasang standar serta prosedur jalannya sebuah CA sampai dengan standar pengamanannya sehingga pemerintah seharusnya tidak hanya diam terpaku, namun mencari cara agar CA yang bermasalah tersebut tidak tutup pada akhirnya, mengingat begitu banyak peran dan jasa dari CA tersebut.

b. Tanggung jawab perdata

Perbuatan yang dilakukan CA tersebut dengan tidak memiliki sistem pengamanan yang ter-*update* sehingga membuatnya dapat diretas oleh *hacker* dan mengakibatkan kebocoran data atau informasi yang dimiliki oleh konsumen CA tersebut merupakan kelalaian yang tidak dapat ditolerir. Mengingat begitu pentingnya data atau informasi tersebut, maka CA dalam hal ini bertanggung jawab penuh atas

tindakan yang telah dilakukannya dengan mencari alternatif lain untuk menarik sertifikat yang telah dikeluarkan oleh CA tersebut.

c. Tanggung jawab pidana

Ganti rugi memang merupakan hal yang utama dalam tanggung jawab ini, namun apabila dana yang tidak mencukupi maka mempailitkan sebuah CA adalah alternatif terakhir yang diambil. Dalam hal ini, seharusnya ada pihak lain yang ikut serta menanggung, bukan hanya CA tersebut saja, melainkan pihak yang membuat s*oftware* sistem pengamanan, *Root* CA, serta pemerintah pun ikut serta dalam tanggung jawab ini sehingga CA tersebut masih dapat bertahan dan melaksanakan tugasnya sebagai CA seperti sebelum adanya kasus peretasan tersebut terlepas nantinya akan adanya ketidakpercayaan dalam diri konsumen terhadap CA itu, namun setidaknya CA yang telah berdiri lama ini patut diperhitungkan peran dan jasa yang telah diberikannya.

4.2. Saran

Adapun saran yang dapat diberikan, yaitu:

1. Diperlukannya sistem pengamanan melalui teknik kriptografi, menerapkan *secured communication* (CIAANA), sumber daya manusia yang handal dan terpercaya serta manajemen yang baik dalam penyelenggaraan sertifikasi elektronik sehingga dapat terhindar dari ancaman dan resiko yang ada dengan cara mengikuti segala prosedur dan standarisasi seperti adanya standar kelaikan penyelenggara sertifikasi elektronik dan *trustworthiness* pada CA.
2. Berdasarkan dengan kasus DigiNotar ini, Indonesia yang telah menggunakan CA asing dan adanya CA swasta memerlukan konsepsi hukum yang baru dengan cara merevisi Peraturan Menteri Komunikasi dan Informatika Nomor 30/Perm./M.KOMINFO/11/2006 mengenai badan pengawas CA karena dianggap kurang memenuhi standar dalam mengawasi serta menjalankan CA sehingga diperlukan penambahan dalam beberapa hal, seperti:
    a. Prosedur pelaksanaan CA secara terperinci dan jelas,

b. Standarisasi kelaikan CA mengikuti standarisasi yang telah ada di negara-negara berkembang yang telah memiliki CA seperti Belanda,
c. Tugas dan peranan CA secara terperinci dan jelas,
d. Tanggung jawab CA, serta
e. Tanggung jawab pemerintah dalam proses pelaksanaan CA,

DAFTAR PUSTAKA

I. PERATURAN PERUNDANG-UNDANGAN

Indonesia, Undang-Undang Tentang Informasi dan Transaksi Elektronik, UU No.11/2008, LN. No. 58 Tahun 2008, TLN No. 4843.

Indonesia, Undang-Undang Tentang Perlindungan Konsumen. UU No.5/1999, LN. No. 42 Tahun 1999, TLN No. 3821.

Indonesia, Peraturan Menteri Komunikasi dan Informatika Tentang Badan Pengawas Certification Authorithy, Permen No. 30/PERM/M.KOMINFO/11/2006.

Indonesia, Rancangan Peraturan Pemerintah Tentang Penyelenggaraan Sistem Elektronik di Instansi Pemerintah Pusat dan Daerah (*E-Government*), 2009.

Indonesia, Rancangan Peraturan Pemerintah Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, 2012.

II. BUKU

Adams, Carlisle dan Steve Lyoyd. *Understanding Public Key Infrastructure.* USA: Macmillan Technical Publishing, 1999.

Ahmad Zein, Yahya. *Kontrak Elektronik & Penyelesaian Sengketa Bisnis E-Commerce*. Bandung: Mandar Maju, 2009.

Budiono, Herlien. *Kumpulan Tulisan Hukum Perdata Di Bidang Kenotariatan*. Bandung: PT.Citra Aditya Bakti, 2007.

Burhan Ashshofa, *Metode Penelitian Hukum,* (Jakarta: Rineka Cipta, 1998)

Chandra, Gregorius, Fandy Tjipto dan Yanto Chandra, *Pemasaran global: Internasionalisasi dan Internetisasi*. Yogyakarta: Andi, 2004.

Halim, Abdul dan Barkatullah Teguh Prasetyo. *Bisnis E-commerce Study System Keamanan dan Hukum di Indonesia*. Yogyakarta: Pustaka Pelajar, 2006.

H.R., Ridwan. *Hukum Administrasi Negara*. Jakarta: Raja Grafindo Persada, 2006.

Makarim, Edmon. *Notaris dan Tanda Tangan Elektronik. Cetakan Pertama.* Jakarta: PT. Rajawali Grafindo Persada, 2011.

Makarim, Edmon. *Pengantar Hukum Telematika*. Jakarta: PT RajaGrafindo Persada, 2005.

Makarim, Edmon. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik.* Jakarta: PR Rajagrafindo Persada, 2010.

Partodiharjo, Soemarno. *Tanya Jawab Sekitar Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.* Jakarta: PT. Gramedia Pustaka Utama, 2009.

Raharjo, Satjipto. *Masalah Penegakan Hukum*. Bandung: Sinar Baru, 1983.

Rahman, Hasanuddin. *Seri Keterampilan Merancang Kontrak Bisnis, Contract Drafting*. Bandung: PT. Citra Aditya Bakti, 2003.

Schellekens, M.H.M. *Electronic Signatures*, Belanda: Cambridge University Press, 2004.

Shidarta, *Hukum Perlindungan Konsumen Indonesia, Edisi Revisi*. Jakarta: Gramedia Widiasarana Indonesia, 2006.

Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Jakarta: Penerbit UI Press, 2006.

Vollmar. *Pengantar Studi Hukum Perdata, Jilid II*. Jakarta: Raja Grafindo Persada, 1998.

W. Purbo, Onno dan Aang Arif Wahyudi. *Mengenal E-Commerce*. Jakarta: PT. Elex Media Komputindo, 2001.

III. JURNAL

Agus Riswandi, Budi. "Aspek Perlindungan Nasabah dalam Sistem Pembayaran Internet", *Jurnal Hukum Lus Wuila Iustu*, Fakultas Hukum Universitas Islam Indonesia, 2002.

Direktorat Jenderal Perdagangan Dalam Negeri Departemen Perindustrian dan Perdagangan Jakarta dan Lembaga Kajian Hukum dan Teknologi Fakultas Hukum Universitas Indonesia, *Naskah Akademik Rancangan Undang-Undang Tentang Tanda Tangan Elektronik dan Transaksi Elektronik*, Jakarta. 2001.

Khairandy, Ridwan, "Pembaharuan Hukum Kontrak Sebagai Antisipasi Transaksi *Elektronic Commerce*", *Jurnal Hukum Bisnis*, Vol. 16, November 2001

Khairandy, Ridwan. "Pengakuan dan Keabsahan Digital Signature dalam Perspektif Hukum Pembuktian", *Jurnal Hukum Bisnis*, Vol.18, Maret 2002.

Remy Sjahdeini, Sutan. "Sistem Pengamanan *E-Commerce*", *Jurnal hukum bisnis* Vol.18, 2002.

IV. SEMINAR/ KUTIPAN

Setiawan, "*Elektronic Commerce*: Tinjauan dari Segi Hukum Kontrak", Disampaikan pada "Seminar *legal Aspect of E-commerce"*, (Jakarta: Agustus 2000).

Suherman, E. "Masalah Tanggung Jawab Pada Charter Pesawat Udara Dan Beberapa Masalah Lain Dalam Bidang Penerbangan (Kumpulan Karangan)", (Bandung: Cet. II Alumni, 1979).

V. INTERNET

Anonim. Diunduh dari http://www.indocybeerlawnet.

Anonim. Diunduh dari http://www.shareilmu.com/public-key-infrastructure.

Anonim. Diunduh dari http://en.wikipedia.org/wiki/Public_key_infrastructure.

Anonim. Siaran Pers No. 44/PIH/KOMINFO/5/2012 tentang Uji Publik RPM Pedoman Umum Audit Sistem Elektronik Penyelenggara Pelayanan Publik, 26 Mei 2012, Diunduh dari http://kominfo.go.id/siaran_pers/detail/2967/Siaran+Pers+No.+44-PIH-KOMINFO-5-2012+tentang+Uji+Publik+RPM+Pedoman+Umum+Audit+Sistem+Elektronik+Penyelenggara+Pelayanan+Publik.

El Said, Fairuz. "Cyber Law-Tanda Tangan Digital", 15 Agustus 2010. Diunduh dari http://fairuzelsaid.wordpress.com/2010/08/24/cyberlaw-konsep-keamanan-sistem-informasi.

Hadiwibowo. "Standar Sistem Manajemen Keamanan Informasi – ISO 17799" Februari 3, 2009. Diunduh dari

Mukti Wibowo, Arianto. "kerangka Hukum *Digital Signature* Dalam *Electronic Commerce"*, 1999, Diunduh dari amwibowo@caplin.cs.ui.ac.id.

Patrianto Tjahjono, Jusuf. "Dengan Berlakunya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dan Tanda Tangan Elektronik", 2008, Diunduh dari www.Legal-hukum.co.id.

Scisco, Peter. "*Electronic Commerce"*, dalam Microsoft Encarta Online, Encyclopedia 2006, Microsoft Corporation 1997-2006, Diunduh dari http://encarta.msn.com.

UNCITRAL. "*Model Law on Electronic Commerce*" 1998, Diunduh dari www.uncitral.org.