ANALISIS FUNGSI DAN PERAN PENYELENGGARA JASA TANDA TANGAN ELEKTRONIK DALAM PERSPEKTIF HUKUM KEARSIPAN DAN DOKUMENTASI PERUSAHAAN

Rizal C. Kusuma

Abstrak

The service of digital signature is created as electronical information system that be aimed to supporting identification by online method's. The digital signature does not same as conventional model which then be migrated into ditigized image and as like signature that's wrote at hard ware which is on touch screen base. The digital signature be resulted of encryption process to electronic models which has been done in mathematical or electronical base and been sent by hard ware connection to any cyberspace network. This approach also runs to particular purpose as reflection of approval beside to protecting towards substance of document and archive of substance changing done. The author explains in the Indonesian legal circumstance's for fruther implication the topic submitted here in the related legal aspects on the role and function of signature digital service, corporate document, and consumer protection.

Kata kunci: hukum perusahaan, fungsi dan peran, jasa, tandatangan elektronik

I. Pendahuluan

Di Indonesia, pemanfaatan teknologi informasi dan komunikasi memiliki peranan yang sangat penting dalam menuju perubahan perilaku hidup masyarakat Indonesia, misalnya melalui pemanfaatan media internet, yang memungkinkan didapatkannya informasi terkini yang diinginkan secara cepat dan mudah.[1]

Hal ini sejalan dengan pertimbangan Pemerintah bahwa pemanfaatan teknologi komunikasi dan informasi dalam proses pemerintahan (*e-government*) akan meningkatkan efisiensi, efektifitas, transparansi dan

---

[1] *Swasta Agar Dilibatkan Percepat CAP* (*Community Access Point*). Bisnis Indonesia, 15 Juni 2004. Yang menulis tentang pengguna internet di Indonesia pada tahun 2000 mencapai 2.000.000 dan pada tahun 2004 mencapai 12.000.000.

akuntabilitas penyelenggaraan pemerintah agar tercapai cita-cita untuk menyelenggarakan pemerintahan yang baik (*good governance*).

Seiring dengan hal itu, notaris merupakan pejabat yang memegang jabatan tertentu yang menjalankan profesi dalam pelayanan hukum kepada publik,[2] lembaga notariat hadir sejak Indonesia dijajah Belanda, semula lembaga notariat diperuntukkan bagi golongan Eropa terutama dalam bidang hukum perdata, namun tidak ada larangan bagi masyarakat Indonesia untuk turut menikmatinya pada saat itu sehingga keberadaannya semakin dibutuhkan di tengah-tengah masyarakat.[3] Hal ini juga seiring dengan dinamika masyarakat yang membutuhkan keberadaan pihak ketiga untuk menetukan apa yang mereka transaksikan sesuai dengan hukum yang berlaku.

Eksistensi notaris yang telah diatur oleh Undang-Undang Tentang Jabatan Notaris UU Nomor 30 Tahun 2004 makin diperluas lagi melalui pendapat majelis Hakim Konstitusi yang menyatakan bahwa notaris merupakan suatu profesi dan pejabat umum yang melaksanakan sebagian dari tugas pemerintah.[4]

Berdasarkan fakta tersebut, maka Notaris di Indonesia perlu mengenal, memahami dan memanfaatkan serta turut mengambil peran serta aktif guna pengembangan teknologi informasi dan komunikasi masa kini yang telah hadir di tengah-tengah masyarakat dunia pada umumnya dan Indonesia pada khususnya dalam rangka mendukung kinerja profesi notaris memberikan pelayanan hukum kepada publik maupun sebagai pejabat umum yang melaksanakan sebagian dari tugas pemerintah.

Dokumen-dokumen hasil dari pelaksanaan tugas notaris, baik dokumen dalam wujud *hardcopy* maupun *softcopy* harus disimpan secara baik dan benar. Sebab berdasarkan Instruksi Presiden nomor 6 tahun 2001 tentang Pengembangan dan Pendayagunaan Telematika di Indonesia dan nomor 3 tahun 2003 tentang Kebijakan dan Strategi Nasional pengembangan *e-Government* yang meletakkan *electronic record* (*e-record*) *management* sebagai dasar penyelenggaraan *e-Government*.[5] Oleh karena itu notaris

---

[2] Indonesia (b), *Undang-Undang Tentang Jabatan Notaris*. UU No. 30. LN No. 117 Tahun 2004, Konsiderans huruf c.

[3] Nico, "Tanggung Jawab Notaris selaku Pejabat Umum", (Yogyakarta: CDSBL, 2003) hal. 35.

[4] Thoso Priharnowo, *Mahkamah Konstitusi Tolak Keberagaman Organisasi Notaris*, Tempointeraktif Selasa, 13 September 2005. <http://www.tempointeraktif.com/hg/hukum/2005/09/13/brk,20050913-66523,id.html>, diakses tanggal 25 Nopember 2005.

sebagai pejabat berkewajiban membenahi dokumen-dokumennya sebagai suatu kesatuan yang integral dengan sistem informasinya.

A. Pokok Permasalahan

Berdasarkan uraian tersebut, permasalahan pokok yang akan diteliti dalam penulisan tesis ini adalah sebagai berikut.

1. Bagaimana fungsi dan peran penyelenggaraan jasa tanda tangan elektronik?
2. Bagaimana analisis hukum terkait penyelenggaraan jasa tanda tangan elektronik dalam perspektif hukum kearsipan dan dokumentasi perusahaan?
3. Bagaimana pertanggungjawaban penyelenggaraan jasa tanda tangan elektronik dalam perspektif hukum perlindungan konsumen?

B. Metode Penelitian

Penelitian adalah suatu kegiatan ilmiah yan seksama, penuh ketekunan dan tuntas terhadap suatu hal–hal tertentu dengan tujuan untuk mengembangkan ilmu pengetahuan manusia. Penelitian juga merupakan sarana untuk mengembangkan ilmu pengetahuan yang menyangkut kegiatan–kegiatan menganalisa dan menggunakan metode yang sistematis dan konsisten terhadap suatu cara tertentu.[6]

Dalam rangka penulisan tesis ini, metode penelitian yang dilakukan dan dipergunakan adalah:

1. Jenis dan Pendekatan Penelitian

Jenis penelitian yaitu penelitian hukum normatif atau penelitian hukum doktriner. Karena penelitian ini dilakukan atau ditujukan terhadap peraturan–peraturan yang tertulis atau hukum positif serta bahan–bahan hukum yang lain, yang berkaitan dengan permasalahan.

Sedangkan pendekatan penelitian yang dilakukan adalah penelitian kepustakaan. Karena di dalam penelitian ini, pengumpulan data dilakukan dengan studi kepustakaan /studi dokumen yang lebih

---

[5] Departemen Komunikasi dan Informasi, *Keputusan Menteri Komunikasi dan Informasi Tentang Panduan Manajemen Sistem Dokumen Elektronik*, Kepmen No. 56/KEP/M.KOMINFO/12/2003.

[6] Soerjono Soekanto, "Pengantar Penelitian Hukum", Cet.III (Jakarta: UI–Press, 1986), hal. 3.

banyak dilakukan terhadap data yang bersifat sekunder yang terdapat di perpustakaan.

2. Sifat Penelitian

Penelitian ini bersifat eksplanatoris, yaitu merupakan suatu penelitian yang bersifat menerangkan, memperkaut atau menguji, dan bertujuan untuk mencari hubungan–hubungan yang ada antara berbagai variabel yang diteliti atau menguji ada tidaknya hubungan tersebut.

3. Sumber dan lokasi penelitian

Sumber dan lokasi penelitian yaitu data sekunder yang meliputi bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier yang terdapat di perpustakaan, karena untuk memperoleh data sekunder tersebut lebih banyak terdapat di perpustakaan.

4. Alat pengumpulan data dan metode–metode pendekatan dalam analisis data

Alat pengumpulan data yang dipergunakan untuk memperoleh data yang diperlukan yaitu studi dokumen, yang meliputi bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Adapun yang dimaksud bahan hukum primer yaitu bahan–bahan hukum yang bersifat mengikat; bahan hukum sekunder yaitu bahan–bahan hukum yang memberikan penjelasan mengenai bahan hukum primer; dan bahan hukum tersier yaitu bahan–baan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer maupun bahan hukum sekunder. Sedangkan metode pendekatan dalam analisis data adalah metode kualitatif, yaitu dengan menyajikan dalam bentuk uraian dan konsep.

II. Peranan Profesi Notaris Bagi Masyarakat

Notaris merupakan salah satu anggota profesi hukum yang bekerja bahu membahu dengan profesi lain. Keberadaan notaris tidak dapat dilepaskan dari peran anggota profesi lainnya yang terlibat dalam upaya penegakan keadilan (*pro justitia*), seperti hakim, jaksa, advokat, Polri, yang selama ini eksis dalam sistem peradilan. Prof. Mr. Paul Scholten berpendapat bahwa para notaris dapat menyumbang dalam pembentukan hukum

(rechtsvorming) karena notaris adalah praktisi dalam menangani Undang-Undang Hukum Perdata dan mempunyai kontak langsung dengan publik.[7]

Di Indonesia, kedudukan hukum notaris tidak dapat dilepaskan dari sistem peradilan, khususnya sistem pembuktian dalam perkara perdata, dimana akta notaris mempunyai nilai pembuktian lebih tinggi. Sistem peradilan yang dimaksud adalah sistem peradilan yang berlaku di Indonesia sesuai dengan Undang-Undang Nomor 14 tahun 1970 yang kemudian dirubah melalui Undang-Undang Nomor 35 tahun 1999 yang melembagakan empat macam badan peradilan, yaitu badan peradilan umum, badan peradilan agama, badan peradilan militer dan badan peradilan tata usaha negara.[8]

A. Notaris Selaku Pejabat Umum Yang Disumpah

Sebelum menjalankan jabatannya, notaris terlebih dahulu mengucapkan sumpah/janji menurut agamanya dihadapan Menteri atau pejabat yang ditunjuk untuk itu.[9]

Dengan tanpa mengurangi makna sumpah/janji tersebut secara komprehensif, terdapat satu alinea yang menyatakan "Bahwa saya akan menjalankan jabatan saya dengan amanah, jujur, saksama, mandiri, dan tidak berpihak." Penjelasan atas Pasal 4 hanya dinyatakan cukup jelas.[10] Sehingga penulis melakukan penafsiran secara gramatikal bahwa notaris adalah pejabat umum yang layak dipercaya *(trusted)* oleh masyarakat luas karena ia akan selalu amanah, jujur, saksama, mandiri, dan tidak berpihak.

B. Tugas Dan Wewenang Notaris Sebagai Pejabat Umum

Pasal 15 Undang-undang Nomor 30 tahun 2004, tentang jabatan Notaris menyatakan bahwa:

---

[7] Tan Thong Kie, "Studi Notariat Beberapa Mata Pelajaran dan Serba-serbi Praktek Notaris", (Jakarta: Ichtiar Baru Van Houve, 2000), hal. 171.

[8] Indonesia (e), *Undang-Undang Tentang Ketentuan-Ketentuan Pokok Kekuasaan Kehakiman*, UU No. 14, LN No. 74 Tahun 1970 TLN No. 2951, lihat juga Indonesia (f), *Undang-Undang Tentang Perubahan Atas Undang-Undang Nomor 14 Tahun 1970 Tentang Ketentuan-Ketentuan Pokok Kekuasaan Kehakiman*, UU No. 35, LN No. 147 Tahun 1999 TLN No. 3879.

[9] Indonesia (c), Pasal 4.

[10] *Ibid.*, Penjelasan Pasal 4.

> *"Notaris berwenang membuat akta otentik mengenai semua perbuatan, perjanjian dan ketetapan yang diharuskan oleh peraturan perundang–undangan dan/atau yang dikehendaki oleh yang berkepentingan untuk dinyatakan dalam akta otentik menjamin kepastian tanggal, pembuatan akta, menyimpan akta memberikan grosse salinan dan kutipan akta, semuanya itu sepanjang pembuatan akta–akta itu tidak juga ditugaskan atau dikecualikan kepada pejabat lain atau orang lain yang ditetapkan oleh undang-undang".*

Tugas dan wewenang Notaris ini erat hubungannya dengan perjanjian–perjanjian, perbuatan–perbuatan dan ketetapan–ketetapan yang menimbulkan hak dan kewajiban antara para pihak, yaitu memberikan jaminan atau alat bukti terhadap perbuatan, perjanjian dan ketetapan–ketetapan tersebut agar para pihak yang terlibat di dalamnya mempunyai kepastian hukum.

Wewenang utama dari notaris adalah membuat suatu akta otentik, sehingga keotentisitasan suatu akta notaris bersumber Pasal 1868 K.U.H. Perdata. Suatu akta otentik disebut memenuhi otentisitas apabila memenuhi 2 unsur yaitu:

1. Akta itu dibuat dalam bentuk yang ditentukan oleh undang-undang;

   Bentuk yang ditentukan oleh undang-undang adalah bahwa akta tersebut terdiri dari kepala akta, badan akta, dan akhir akta. Bagian–bagian akta yang terdiri dari kepala akta dan akhir akta adalah bagian yang mengandung unsur otentik, artinya apa yang tercantum dalam kepala akta dan akhir akta tersebut akan menentukan apakah akta itu dibuat dalam bentuk yang ditentukan undang-undang atau tidak.
2. Akta dibuat oleh (*door*) atau di hadapan (*ten overstaan*) seorang pejabat umum;

   Apabila akta notaris hanya memuat apa yang dialami dan disaksikan oleh notaris sebagai pejabat umum, maka akta itu dinamakan akta verbal atau akta pejabat (*ambtelijk akte*). Salah satu contoh akta pejabat ialah berita acara yang dibuat oleh notaris dari suatu rapat pemegang saham dari suatu perseroan terbatas. Apabila suatu akta selain memuat tentang apa yang diperjanjikan atau ditentukan oleh pihak–pihak yang menghadap pada notaris, maka akta itu dinamakan akta partij atau akta para pihak.

Adapun perbedaan sifat dari dua macam akta tersebut adalah:

1) Akta pejabat masih sah dipakai sebagai alat bukti apabila ada satu atau lebih di antara para pihak tidak menandatangani dan Notaris menyebutkan dalam akta tersebut apa penyebab mereka tidak menandatangani akta tersebut.[11]
2) Akta *partij* tidak akan berlaku sebagai alat bukti apabila salah satu pihak tidak menandatangai akta karena hal tersebut dapat diartikan bahwa ia tidak menyetujui perjanjian yang dibuat, kecuali apabila alasan tidak menandatangani itu adalah alasan yang kuat seperti tidak bisa tulis menulis (bisa dengan cap jempol) atau tangannya sakit, dan lain sebagainya. Alasan seperti itu harus dicantumkan dengan jelas oleh Notaris dalam akta yang bersangkutan.[12]

Salah satu syarat yang harus dipenuhi agar suatu akta memperoleh otentisitas adalah kewenangan Notaris yang bersangkutan untuk membuat akta tersebut. Kewenangan tersebut meliputi empat hal, yaitu:

1. Notaris berwenang sepanjang menyangkut akta yang dibuatnya;
2. Notaris berwenang sepanjang mengenai orang untuk kepentingan siapa akta itu dibuat;
3. Notaris berwenang sepanjang mengenai tempat di mana akta dibuat;
4. Notaris berwenang sepanjang mengenai waktu pembuatan akta.[13]

Apabila salah satu hal diatas tidak dipenuhi, maka akibatnya akta yang bersangkutan bukan merupakan akta otentik dan hanya berlaku sebagai akta yang dibuat di bawah tangan sepanjang akta tersebut ditandatangani oleh para pihak.[14]

Disamping tugas–tugas yang ditentukan dalam Pasal 15 (2) Undang-undang Jabatan Notaris tersebut di atas dalam prakteknya notaris juga melayani masyarakat untuk:

1. Mengesahkan tanda tangan dan menetapkan kepastian tanggal surat di bawah tangan dengan mendaftar dalam buku khusus
2. Membukukan surat–surat di bawah tangan

---

[11] *Ibid.*, hal. 53.

[12] *Ibid.*, hal. 52.

[13] *Ibid.*, hal. 49.

[14] *Ibid.*, hal. 50.

3. Membuat kopi dari asli surat–surat di bawah tangan berupa salinan yang memuat uraian sebagaimana ditulis dan digambarkan dalam surat yang bersangkutan
4. Melakukan pengesahan kecocokan fotokopi dengan surat aslinya
5. Memberikan penyuluhan hukum sehubungan dengan pembuatan akta
6. Membuat akta yang berkaitan dengan pertanahan; atau membuat akta risalah lelang.

C. Praktek Notaris Dalam Lingkup Legalisasi

Dalam praktek sering ditemukan surat–surat di bawah tangan dilegalisasi oleh pejabat yang tidak berwenang untuk itu, misalnya oleh Lurah. Legalisasi yang diperbuatnya itu tidak sesuai dengan legalisasi yang ditetapkan oleh undang-undang, bahkan sering juga oleh pejabat tertentu dilegalisasi surat di bawah tangan yang tanggal penandatanganannya berbeda, hal ini jelas tidak sesuai dengan maksud dan tujuan legalisasi.

Sebagian masyarakat berpendapat bahwa dengan dilegalisasinya surat di bawah tangan itu, surat itu memperoleh kedudukan sebagai akta otentik dengan perkataan lain surat itu dianggap seolah–olah dibuat oleh atau dihadapan Notaris. Pendapat tersebut adalah salah, oleh karena surat demikian, sekalipun itu telah dilegalisasi, tetap merupakan surat yang dibuat di bawah tangan.

Wewenang untuk legalisasi surat di bawah tangan tidak hanya diberikan kepada notaris akan tetapi juga kepada beberapa pejabat lainnya, yaitu Ketua Pengadilan Negeri, Walikota atau Bupati.[15]

Pejabat–pejabat tersebut membubuhkan tanggal dan keterangan di bagian bawah dari surat itu yaitu dicantumkan suatu keterangan yang berbunyi:[16]

> *Saya, yang bertanda tangan di bawah ini, ..., Notaris (atau salah satu pejabat tersebut) di ... menerangkan bahwa isi surat ini telah saya bacakan dan terangkan kepada .... yang saya, notaris (atau salah satu pejabat tersebut) kenal/diperkenalkan kepada saya. notaris (atau salah satu pejabat tersebut) dan sesudah itu maka ... tersebut*

---

[15] M.U. Sembiring, "Tehnik Pembuatan Akta", (Medan: Program Pendidikan Spesialis Notariat Fakultas Hukum Universitas Sumatra Utara, 1997) hal. 125.

[16] Tobing. *Op. Cit.*, hal. 228.

membubuhkan tanda tangan / cap jarinya di atas surat ini di hadapan saya, notaris (atau salah satu pejabat tersebut).

Perbedaan surat di bawah tangan yang dilegalisasi oleh pejabat yang berwenang dengan surat di bawah tangan yang tidak dilegalisasi adalah, bahwa surat di bawah tangan yang dilegalisasi mempunyai tanggal yang pasti, tanda tangan yang dibubuhkan di bawah surat itu benar berasal dan dibubuhkan oleh orang yang namanya tercantum dalam surat itu dan orang yang membubuhkan tanda tangannya di bawah surat itu, tidak dapat mengatakan, bahwa ia tidak mengetahui apa isi surat itu, oleh karena isinya telah terlebih dahulu dibacakan kepadanya, sebelum ia membubuhkan tanda tangannya di hadapan pejabat itu.[17]

D. Fungsi Legalisasi Dan Kekuatan Pembuktian Akta Di Bawah Tangan Yang Telah Memperoleh Legalisasi Dari Notaris

Akta di bawah tangan yang telah memperoleh legalisasi memberikan kepastian bagi hakim mengenai tanggal dan identitas dari para pihak yang mengadakan perjanjian tersebut serta tanda tangan yang dibubuhkan di bawah surat itu benar berasal dari dan dibubuhkan oleh orang yang namanya tecantum dalam surat itu dan orang yang membubuhkan tanda tangan dibawah surat itu tidak lagi dapat mengatakan bahwa para pihak; atau salah satu pihak tidak mengetahui apa isi surat itu, karena isinya telah dibacakan dan dijelaskan terlebih dahulu sebelum para pihak membubuhkan tanda tangannya di hadapan Notaris itu.

Menurut ketentuan Pasal 1880.KUHPerdata akta–akta di bawah tangan yang tidak dilegalisasi oleh Notaris atau pejabat lain yang ditunjuk oleh atau berdasarkan undang-undang Pasal 1874 dan Pasal 1874 a KUHPerdata mengenai tanggalnya tidak mempunyai kekuatan terhadap pihak ketiga (*derden*) selainnya atau kecuali:

1. Sejak hari legalisir yang dimaksud tersebut dan dibukukannya menurut undang-undang; atau
2. Sejak hari meninggalnya penandatangan yang bersangkutan baik semuanya atau salah seorang; atau
3. Sejak hari dibuktikan tentang adanya akta di bawah tangan itu dari akta–akta yang dibuat oleh pegawai umum; atau

---

[17] Sembiring, *Op. Cit.*, hal. 129–130.

4. Sejak baru diakuinya akta di bawah tangan itu secara tertulis oleh pihak ketiga terhadap akta itu dipergunakan.

Kekuatan pembuktian materil akta di bawah tangan menurut Pasal 1875 KUHPerdata, oleh orang terhadap akta itu digunakan atau yang dapat dianggap diakui menurut undang-undang bagi yang menandatangani ahli warisnya serta orang–orang yang mendapat haknya dari orang tersebut, merupakan bukti sempurna seperti akta otentik.

Berdasarkan hal tersebut, maka akta di bawah tangan yang telah memperoleh legalisasi dari Notaris mempunyai kekuatan pembuktian yang sempurna, karena akta di bawah tangan kebenarannya terletak pada tanda tangan para pihak. Jadi dengan diakuinya tanda tangan tersebut, maka isi akta pun dianggap sebagai kesepakatan para pihak.

E. Kekuatan Pembuktian Akta Di Bawah Tangan Di Dalam Proses Pemeriksaan Perkara Di Pengadilan

Menurut definisi Prof. Mr. A. Pitlo, alat pembuktian adalah "Pembawa tanda tangan bacaan yang berarti, menerjemahkan suatu isi pikiran." Alat bukti tulisan ini menurut doktrin ilmu hukum dan undang-undang secara garis besar dibagi 2 macam:[18]

1. Tulisan biasa
2. Tulisan yang berupa akta.

Tulisan yang berupa akta ini dibagi menjadi 2, yaitu:

1. akta di bawah tangan
2. akta otentik

Dengan pembuktian akan dapat ditentukan kebenaran menurut hukum serta dapat menjamin perlindungan terhadap hak–hak para pihak yang berperkara secara seimbang.

Khusus dalam perkara Perdata telah ditentukan, bahwa tidak semua peristiwa atau kejadian harus dibuktikan, melainkan hanya hal–hal yang menjadi perselisihan saja yang harus dibuktikan.

Akta otentik merupakan alat bukti yang paling kuat nilai pembuktiannya, bahkan dikatakan mempunyai kekuatan pembuktian

---

[18] Wicaksono Wahyu Santoso. *Keberadaan RUU Tanda Tangan Digital Dan Transaksi Elektronik Kaitannya dengan Kesiapan Masyarakat Pelaku Usaha dan Sistem Penegakan Hukum*. Ikhtnet 31 Juli 2004. <http://Ikht.net /artikel_lengkap.php?id=14>. diakses tanggal 3 Juli 2006.

yang "sempurna" atau "lengkap" yang berarti mengikat dan harus diakui hakim sebagai kebenaran menurut hukum, kecuali terbukti sebaliknya, misalnya karena ada kepalsuan dalam akta otentik tersebut.

Jadi akta di bawah tangan hanya dapat diterima sebagai permulaan bukti tertulis (Pasal 1871 KUHPerdata) namun menurut Pasal tersebut tidak dijelaskan apa yang dimaksud dengan bukti tertulis itu.

Di dalam Pasal 1902 KUHPerdata dikemukakan syarat–syarat bilamana terdapat permulaan bukti tertulis, yaitu:[19]

1. Harus ada akta;
2. Akta itu harus dibuat oleh orang terhadap siapa dilakukan tuntutan atau dari orang yang diwakilinya;
3. Akta itu harus memungkinkan kebenaran peristiwa yang bersangkutan.

III. *Electronic Record Management* Dalam Hukum Kearsipan Dan Dokumentasi

A. Konsep *Certification Authority*

Pemanfaatan media elektronik *(internet)* untuk menunjang transaksi perniagaan elektronik *(e-Commerce)* telah berkembang secara cepat. *E-Commerce* bukan saja telah menjadi *main-stream* budaya negara-negara maju tetapi juga telah menjadi model transaksi negara-negara lain termasuk Indonesia. Namun kegiatan-kegiatan *e-Commerce* dalam jaringan *internet* yang seringkali disebut sebagai dunia maya *(virtual world)* telah menyebabkan timbulnya kebutuhan penggunaan sertifikat elektronik (SE) untuk mengamankan pertukaran informasi serta memberikan kepastian hukum bagi para pihak yang melakukan transaksi melalui media elektronik *(internet)*.[20]

Suatu pertukaran informasi melalui media elektronik (*internet*) yang terkait dengan transaksi bisnis atau perdagangan secara elektronik, memerlukan pengamanan melalui infrastruktur kunci publik *(Public Key Infrastructure)* agar informasi yang dipertukarkan hanya bisa dibaca oleh penerima yang berhak dan tidak dapat dipahami oleh pihak yang tidak berhak *(Privacy/Confidentiality)*,

---

[19] Notodisoerjo. *Op. Cit.*, hal. 44.

[20] Indonesia (m). *Rancangan Peraturan Menteri Komunikasi dan Informatika tentang Pedoman Penyelenggaraan Certification Authority di Indonesia*, Pendahuluan.

identitas pihak yang terkait dapat diketahui atau dijamin otentisitasnya *(Authentification)*, informasi yang dikirim dan diterima tidak berubah *(Integrity)*, dan pihak yang terkait tidak dapat menyangkal telah melakukan transaksi *(Non Repudiation)*.

Pengamanan terhadap informasi (pesan) yang dikirim dalam suatu transaksi melalui media elektronik menempati tataran paling tinggi dan sangat penting. Fakta menunjukkan perubahan pesan-pesan eletronik dapat dilakukan dengan mudah dan tidak terdeteksi, sehingga meningkatkan resiko terjadinya manipulasi terhadap pesan elektronik yang dikirim. Meningkatnya penggunaan jaringan komunikasi terbuka *(internet)*, akan meningkatkan pula resiko kecurangan, penipuan serta akses ilegal.

Hal-hal di atas menyebabkan diperlukannya sistem dan prosedur pengamanan yang handal, dalam konteks penggunaan sistem komunikasi dengan jaringan terbuka (*internet*), agar timbul kepercayaan dan kepastian hukum bagi pengguna terhadap sistem komunikasi tersebut. Tindakan pencegahan untuk mengelola resiko tersebut termasuk penggunaan infrastruktur kunci publik, mensyaratkan keterlibatan pihak ketiga terpercaya *(Trusted Third Party)* dan independen.

Pihak ketiga terpercaya akan membantu menjamin identitas dari para pihak pelaku transaksi elektonik melalui infrastruktur kunci publik dan menyediakan mekanisme untuk melakukan transaksi elektronik secara aman. Selanjutnya pihak ketiga terpercaya akan memberikan layanan tersebut melalui suatu institusi yang lazim dikenal sebagai *Certification Authority* (CA). CA menerbitkan SE dalam bentuk Sertifikat Digital (SD) - (*Digital Certificate*) yang digunakan para pihak untuk menyatakan identitasnya dalam melakukan transaksi elektronik.

Dalam tingkatan CA yang lebih tinggi, dibutuhkan notaris untuk lebih memastikan identitas si penanda tangan.[21]

B. Konsep *Public Key Infrastructure*

Dalam sistem kriptografi, *public key infrastructure* (PKi) adalah suatu bentuk pengaturan yang menyediakan dokumen *track record*,

---

[21] "*Notaries are required in some cases to personally know the party whose signature is being notarized; this is a higher standard than can be reached for many Cases*". <http://en.wikipedia.org/wiki /Certificate_authority>, diakses pada tanggal 20 Juli 2006.

identitas pengguna dan pernyataan keabsahan identitas bagi pihak ketiga terpercaya.[22]

Public Key Infrastructure berfungsi untuk memfasilitasi *digital signature* sebagai *Public Key* dan pengacakannya atau enkripsi sebagai *Private Key*. Analogi dari kedua fungsi ini adalah seperti halnya penerbitan kartu ATM selalu terdiri dari sepasang kunci pertama adalah nomor kartu atau *Public Key* yang bisa diberikan kepada publik yang kedua adalah nomor PIN (*Private Key*) yang hanya diketahui oleh si pemegang kartu saja.

C. Pengaturan Hukum Mengenai Manajemen Dokumen

Di Indonesia, yang menjadi dasar hukum pengaturan *Electronic Document*, ialah:

1. Keputusan Presiden R.I. Nomor 228/M Tahun 2001 tentang Susunan Kabinet Gotong Royong;
2. Keputusan Presiden R.I. Nomor 101 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi dan Tata Kerja Menteri Negara, sebagaimana telah beberapa kali diubah terakhir dengan Keputusan Presiden R.I. Nomor 47 Tahun 2003;
3. Keputusan Presiden R.I. Nomor 9 Tahun 2003 tentang Tim Koordinasi Telematika Indonesia;
4. Instruksi Presiden R.I. Nomor 6 Tahun 2001 tentang Pengembangan dan Pendayagunaan Telematika di Indonesia;
5. Instruksi Presiden R.I. Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *e-Government*;
6. Keputusan Menteri Negara Komunikasi dan Informasi Nomor: 05/SK/MENEG/KI/2001 tentang Organisasi dan Tata Kerja Kantor Menteri Negara Komunikasi dan Informasi;
7. Keputusan Menteri Negara Komunikasi dan Informasi Nomor: 12/SK/MENEG/KI/2002 tanggal 1 Maret 2002 tentang Pembentukan Organisasi Task Force Pengembangan *e-Government*.

---

[22] <http://en.wikipedia.org/wiki/Public_key_infrastructure>. diakses tanggal 20 Juli 2006.

Dasar pelaksananya antara lain:

1. Instruksi Presiden Republik Indonesia Nomor 6 tahun 2001 tentang Pengembangan dan Pendayagunaan Telematika di Indonesia.
2. Keputusan Presiden RI Nomor 228/M tahun 2001 tentang Pembentukan Kabinet Gotong Royong;
3. Keputusan Presiden RI nomor 101 tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Menteri Negara;
4. Kerangka kerja Teknologi Informasi Nasional (*National IT Framework*/NITF).
5. Keputusan Presiden Republik Indonesia Nomor 9 Tahun 2003 tentang Tim Koordinasi Telematika Indonesia.
6. Instruksi Presiden Republik Indonesia No. 3 Tahun 2003, tentang Strategi dan Kebijakan Nasional Pengembangan *E-Government*.

D. Implementasi Sistem *Electronic Record* Management

Mengimplementasikan sistem ERM pada lembaga pemerintah, sehingga pengelolaan dokumen dapat dilakukan dengan lebih efisien. Seperti telah dijelaskan sebelumnya, dokumen elektonik harus memiliki tingkat kepercayaan sebagai sebuah dokumen legal. Dengan diakuinya dokumen elektronik sebagai dokumen legal, maka dokumen elektronik dapat dijadikan bukti/petunjuk riwayat organisasi secara eksplisit. Dalam konteks legal, sebuah bukti dapat berupa dokumentasi, perkataan, audio-visual, baik secara elektronik maupun bentuk lain.

Sebuah dokumen harus memiliki sifat sebagai sesuatu yang utuh dan akurat yang harus memiliki tiga karakteristik utama yaitu:

1. Konten/kandungan: Merupakan informasi yang membangun sebuah dokumen yang dapat berupa kata-kata, gambar, simbol, dan sebagainya.
2. Konteks: Lingkungan di luar konten yang turut serta dalam pembuatan, penerimaan, serta penggunaan sebuah dokumen yaitu lingkungan organisasi, fungsional, dan operasional.
3. Struktur: Format fisik dan logika sebuah dokumen serta hubungan antar elemen di dalamnya.

Dokumen elektronik yang perlu disimpan dan dipelihara dalam jangka waktu yang lama harus memperhatikan kepastian aksesibilitas

dokumen tersebut. Ketentuan tersebut mencakup langkah-langkah pemindaian (*scanning*) dokumen asli (spesifikasi, format file, metadata), pemeliharaan (dokumentasi, duplikasi, dan penyegaran media), serta keberlanjutan keberadaannya.

E. Penyelenggaraan Jasa Tanda Tangan Elektronik Dan Penyelenggaraan Pihak Ketiga Terpercaya (*Trusted Third Party*)

1. Definisi *E-Notary* Dan *Digital Signature* Dalam Sistem Hukum

Indonesia sendiri masih berjalan di tempat dalam hal pengaturan berkenaan dengan praktek *electronic notary* (*e-notary*). Sebab aturan sebagai landasan penyelenggaran *e-notary* masih belum disahkan walaupun Inpres terkait dengan masalah telematika dan *e-Government* sudah mengindikasikan *political will* pemerintah Republik Indonesia. Urgensi pengaturan Anti Penyalahgunaan Komputer yang berkaitan dengan *cybercrime* belum diatur sehingga perlu adanya payung hukum yang eksplisit. Pemerintah melalui Mabes POLRI dan Kejaksaan Agung meminta agar Dewan Perwakilan Rakyat (DPR) segera mengesahkan RUU Informasi dan Transaksi Elektronik (ITE).[23]

E-notary dalam sistem hukum Amerika diartikan sebagai orang yang bertugas untuk menjalankan Undang-Undang Jabatan Notaris.[24] Sedangkan tanda tangan elektronik adalah suatu metode elektronik atau proses melalui aplikasi prosedur keamanan yang mana digunakan untuk menentukan bahwa tanda tangan elektronik pada saat penandatanganan berlangsung:

---

[23] Permintaan itu disampaikan oleh Kepala Badan Reserse dan Kriminal (Bareskrim) Mabes Polri Irjen Pol Makbul Padmanagara dan Jaksa Agung Muda Pidana Umum (Jampidum) HM Prasetyo dalam Rapat Dengar Pendapat Umum dengan Pansus RUU ITE di Gedung DPR, Jl Gatot Subroto, Jakarta, Kamis (18/5/2006). Kabareskrim Polri di depan Pansus yang diketuai oleh anggota FPPP DPR Andi Ghalib mengatakan, akhir-akhir ini teknologi komputer semakin marak digunakan sebagai alat kejahatan. Dicontohkannya beberapa kasus yang bernuansa *cyber crime* yang pernah ditangani Mabes Polri. detikinet.com kamis, 18/05/2006 12:47, diakses tanggal 3 Juli 2006.

[24] *"Electronic notary public" or "electronic notary" means any person commissioned to perform notarial acts.* Lihat <http://www.azleg.state.az.us/ars/41/00351.htm>, diakses tanggal 3 Juli 2006.

1. memiliki identitas yang unik melekat pada pengguna
2. dapat di verifikasi
3. dibawah penguasaan langsung si pengguna
4. berhubungan langsung dengan dokumen yang dimaksud sehingga tanda tangan elektronik bisa batal dengan sendirinya apabila isi dokumen berubah.[25]

Definisi menurut UNCITRAL Uniform Rulers on Electronic Signatures Draft adalah:

> *Data in electronic form in, affixed to, or logically associated with, a data message, and that may be used to identify the signature holder in relation too data message and indicate the signature's holder approval of the information contained in the data message.*[26]

Sedangkan konsep tanda tangan elektronik menurut Rancangan Undang-Undang Republik Indonesia tentang Informasi dan Transaksi Elektronik (RUU ITE) adalah:

> *Informasi elektronik yang dilekatkan, memiliki hubungan langsung atau terasosiasi pada suatu informasi elektronik lain yang dibuat oleh penandatangan untuk menunjukkan identitas dan statusnya sebagai subyek hukum, termasuk dan tidak terbatas pada penggunaan inrastruktur kunci publik (tanda tangan digital), biometrik, kriptografik.*[27]

Seiring dengan pengaturan RUU ITE, Pemerintah melalui Keputusan Menteri Komunikasi dan Informasi (Kepmenkominfo)

---

[25] *Ibid., means an electronic method or process that through the application of a security procedure allows a determination that the electronic signature at the time it was executed was all of the following:*

a. *Unique to the person using it.*
b. *Capable of verification.*
c. *Under the sole control of the person using it.*
d. *Linked to the electronic document to which it relates in a manner so that if the document is changed the electronic signature is invalidated.*

[26] <http://www.uncitral.org/pdf/english/workinggroups/wg_ec/wp-80.pdf>, diakses tanggal 3 Juli 2006.

[27] Indonesia (g). *Rancangan Undang-Undang Republik Indonesia Tentang Informasi dan Transaksi Elektronik.*

nomor: 56/KEP/M.KOMINFO/12/2003 Tentang Panduan Manajemen Sistem Dokumentasi Elektronik memberikan suatu arahan mengenai penandaan yakni:

1. Penanda (*signer*) dapat teridentifikasi, adalah metode yang digunakan untuk mengidentifikasi seseorang dan mengotorisasi untuk menggunakan suatu metode penandaan elektronik tertentu.
2. Pihak penanda terhubung dengan tanda yang bersesuaian, adalah proses, prosedur, dan kebijakan yang menghubungkan pihak penanda dengan informasi dan metode yang digunakan untuk menandai.

Tanda terhubung dengan integritas dari sebuah *record*, maksudnya ialah sebuah tanda elektronik harus terhubung dengan *record* yang bersesuaian, harus ada sebuah metode untuk menjamin bahwa tanda yang dihubungkan dengan suatu isi *record* yang dimaksudkan oleh penanda sedemikian sehingga segala perubahan pada *record* sejak *record* tersebut diberi tanda dapat terdeteksi.

2. Cara Kerja Tanda Tangan Digital

Pasal 1887 KUHPer berbunyi:

> *Tongkat-tongkat berkelar yang sesuai dengan kembarnya, harus dipercaya, jika digunakan antara orang-orang yang biasa membuktikan penyerahan-penyerahan barang yang dilakukannya atau diterimanya dalam jumlah-jumlah kecil, dengan cara yang demikian itu.*

Berdasarkan Pasal diatas, pada masa dahulu manusia telah mengenal proses otentikasi dalam melakukan hubungan perniagaan. Dipergunakan tongkat kayu yang dipatahkan menjadi dua. Jika orang hendak melakukan pencacahan atas suatu transaksi, orang menorehkan sebuah goresan yang menggores sambungan kedua tongkat (yang berpasangan) tersebut. Untuk mencocokkan, cukup dengan menyambungkan kedua tongkat tersebut dan melihat apakah goresan itu 'melintas' sambungan/patahan tongkat dengan baik.[28]

---

[28] Santoso, *op. cit.*

Tanda tangan elektronik menggunakan teknologi yang jauh lebih maju daripada uraian diatas. Tanda tangan elektronik menggunakan *cryptography*, yaitu cabang ilmu matematika terapan dimana dengan menggunakan metode tertentu dapat merubah input data menjadi bentuk yang tidak dapat dimengerti kemudian merubahnya kembali ke bentuk semula. Tanda tangan digital menggunakan kriptografi kunci publik (*public key cryptography*) yang memanfaatkan algoritma dengan menggunakan 2 (dua) kunci matematis yang berbeda namun tetap memiliki keterkaitan. Kunci yang pertama untuk membuat tanda tangan digital atau merubah input data menjadi bentuk yang tidak dapat dimengerti, sedangkan kunci yang kedua untuk memverifikasi tanda tangan digital atau merubah input data menjadi bentuk yang dapat dimengerti.[29]

Kedua uraian singkat diatas memiliki kesamaan bahwa proses otentikasi membutuhkan pasangan (*pairs*) untuk mengenali satu sama lain.

Untuk menjalankan kriptografi kunci publik dibutuhkan peralatan komputer dan perangkat lunak (*software*) yang dapat mengakomodasi dan memanfaatkan kunci-kunci tersebut, yang secara kolektif disebut sistem kriptografi asimetris (*asymmetric cryptosystem*). Kunci pelengkap dari sebuah kunci sistem kriptografi asimetris yang dipergunakan untuk membuat tanda tangan digital biasa disebut dengan istilah kunci pribadi (*private key*), yang mana dimiliki hanya oleh penandatangan untuk membuat tanda tangan digital. Dan kunci publik yang yang secara luas dikenal dan digunakan oleh pihak yang lain untuk memverifikasi tanda tangan tersebut.[30]

Proses ini tidak dijamin 100 (seratus) persen aman. Pengamanan terhadap informasi (pesan) yang dikirim dalam suatu transaksi melalui media elektronik merupakan hal yang sangat penting. Fakta menunjukkan perubahan pesan-pesan eletronik dapat dilakukan dengan mudah dan tidak terdeteksi, sehingga meningkatkan resiko terjadinya manipulasi terhadap pesan elektronik yang dikirim.[31] Meningkatnya penggunaan jaringan

---

[29] American Bar Association Section of Science and Technology Information Security System, *Digital Signature Guidelines Tutorial*, <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>, diakses tanggal 3 Juli 2006.

[30] *Ibid.*

komunikasi terbuka *(internet)*, akan meningkatkan pula resiko kecurangan, penipuan serta akses ilegal. Sehingga dibutuhkan kehadiran pihak lain yang dapat dipercaya. Diperlukannya sistem dan prosedur pengamanan yang handal, dalam konteks penggunaan sistem komunikasi dengan jaringan terbuka (*internet*), agar timbul kepercayaan dan kepastian hukum bagi pengguna terhadap sistem komunikasi tersebut. Tindakan pencegahan untuk mengelola resiko tersebut termasuk penggunaan infrastruktur kunci publik, mensyaratkan keterlibatan pihak ketiga terpercaya *(Trusted Third Party)* dan independen.

Pihak ketiga terpercaya akan membantu menjamin identitas dari para pihak pelaku transaksi elektonik melalui infrastruktur kunci publik dan menyediakan mekanisme untuk melakukan transaksi elektronik secara aman. Selanjutnya pihak ketiga terpercaya akan memberikan layanan tersebut melalui suatu institusi yang lazim dikenal sebagai *Certification Authority* (CA). CA menerbitkan Surat Edaran dalam bentuk Sertifikat Digital (*Digital Certificate*) yang digunakan para pihak untuk menyatakan identitasnya dalam melakukan transaksi elektronik.

Kehadiran CA dalam suatu transaksi elektronik untuk mendukung aspek keamanan dalam mengamankan pertukaran informasi/pesan serta memberikan kepastian hukum dan melindungi para pihak yang melakukan transaksi melalui internet diperlukan sistem dan prosedur pengamanan yang handal dalam konteks penggunaan sistem komunikasi dengan jaringan internet, agar timbul kepercayaan pengguna terhadap sistem komunikasi tersebut.[32]

sebagai suatu institusi baru yang akan memainkan peran penting, diperlukan Pedoman Penyelenggaraan CA di Indonesia yang dapat memberikan penjelasan mengenai pengorganisasian CA, pengawasan penyelenggaraan CA, pengamanan penggunaan CA pada transaksi elektronik, pengamanan infrastruktur CA dan peran pemerintah untuk memberikan kepastian hukum dan melindungi kepentingan masyarakat dari resiko kerugian akibat perbuatan CA yang tidak bertanggung jawab.[33]

---

[31] Jaringan internet memang rawan dengan kejahatan cyber (*cybercrime*), beberapa negara sudah membuat payung hukum agar pelaku *cybercrime* dapat ditindak tegas.

[32] Indonesia (m), Konsiderans huruf b.c.d.

[33] *Ibid.*

3. Institusi Notaris Sebagai *Certification Of Authority*

Peranan penting notaris dalam dunia nyata, dapat dilaksanakan juga dalam dunia maya, yakni mengenai harus mengenal para pihak yang hadir dihadapannya dalam rangka pembuatan suatu akta.[34] Hal tersebut dapat dilakukan dengan meminta identitas dari para penghadap atau meminta keterangan dari orang lain yang dikenalnya. Menurut Pasal 39 Undang-undang Nomor 30 tahun 2004 tentang jabatan Notaris:

1. Penghadap harus memenuhi syarat sebagai berikut :
    1. Paling sedikit berumur 18 (delapan belas) tahun atau telah menikah; dan
    2. Cakap melakukan perbuatan hukum
2. Penghadap harus dikenal oleh Notaris atau diperkenalkan kepadanya oleh 2 (dua) orang saksi pengenal yang berumur paling sedikit 18 (delapan belas) tahun atau telah menikah dan cakap melakukan perbuatan hukum atau diperkenalkan oleh 2 (dua) penghadap lainnya

Pengenalan sebagaimana dimaksud pada ayat (2) dinyatakan secara tegas dalam akta.

Sedapat mungkin Notaris harus berupaya mengikuti bahwa identitas dan keterangan dari para pihak adalah yang sebenarnya. Notaris dapat memperoleh keterangan–keterangan itu dari orang–orang yang dikenalnya dan dipercayainya atau dapat melihat identitas lain seperti paspor, dan surat–surat lain dari para pihak yang bersangkutan, atau melalui informasi dari pihak ketiga.[35]

---

[34] Sembiring. *Op. Cit.*, hal. 69.

[35] *Ibid.*, hal. 71.

IV. Beberapa Kegiatan Praktek Online Notary/E-Notary Dan Trusted Third Party

A. *Genuinedoc*[36]

Genuinedoc menjalankan praktek *online notary* sejak 13 April 2003, ia menawarkan perlindungan dokumen terutama dokumen-okumen yang akan dipublikasikan dalam situs web (*web site*).

Ia juga menawarkan jasa untuk menyakinkan pelanggan, mitra dan pemegang saham dari si pengguna jasa genuinedoc bahwa dokumen yang di publikasi oleh pengguna jasa adalah benar dokumen elektronik dari yang bersangkutan, dengan menerangkan tanggal dokumen itu ketika dipublikasikan.

Apabila ada penggantian dari substansi dokumen tersebut, baik dari si pengguna jasa, orang dalam baik dari pengguna jasa maupun pihak-pihak terkait dan seorang *hacker*[37] memasuki sistem (tidak ada keamanan yang benar-benar aman), *Genuinedoc* akan mendeteksi dan akan memperingatkan sedini mungkin kepada pengguna jasa.

Hal ini dimungkinkan dengan tanda tangan digital maupun dengan memberikan teraan khusus. Ketika pengguna jasa menandai dokumennya, anda menyakini tiap-tiap kata substansi dokumen tersebut. Hal-hal demikian membantu agar hubungan kepercayaan antara klien pengguna jasa, mitra, dan investor menjadi lebih baik.

Penggunaan jasa *Genuinedoc* dilarang untuk tujuan, (1) untuk dan atau atas nama suatu organisasi lain (2) mencoba menipu konsumen dengan merubah penandaan atau teraan khusus pada dokumen. Ketika *Genuinedoc* meminta dokumen tersebut atau mengadakan manipulasi tampilan dari HTML (*Hyper Text Markup Languange*) di dalam dokumen yang sudah ditandai. Termasuk dan tidak terbatas, merubah tampilan warna, huruf, yang dapat menipu konsumen dan membuat konsumen tidak mengenali secara secara benar dokumen yang telah ditandai. (3) segala bentuk penyalahgunaan maksud dan tujuan oleh pengguna jasa. Tiap percobaan untuk menipu konsumen dan atau pihak terkait akan berakibat penghentian segera terhadap *account* pengguna jasa oleh *Genuinedoc*.

---

[36] Lihat situs <http://www.genuinedoc.com/index.html>, diakses tanggal 14 Juli 2006.

[37] *Pengguna tanpa hak yang mencoba untuk mendapatkan akses terhadap suatu system informasi*. Lihat, <www.tecrime.com/0gloss.htm>, diakses tanggal 14 Juli 2006.

Pengguna jasa *Genuinedoc* menerima pengunaan *software* berlisensi berupa *Signdoc* yang bebas royalti (gratis). Penggunaan *software* tersebut semata-mata hanya digunakan bersamaan dengan pemanfaatan jasa *Genuinedoc*, *software Signdoc* dilarang untuk di distribusikan kembali, tidak dapat di sub lisensikan, dan tidak dapat dibatalkan. Lisensi atas penggunaan *Signdoc* tidak dapat diberikan kepada pihak lain, tidak dapat dipindahkan, tidak dapat diperjanjikan untuk dipindahkan, tidak dapat di hipotik/di pasang hak tanggungan dan segala bentuk pembebanan oleh pengguna jasa maupun oleh pihak ketiga.

Genuinedoc tidak menjamin bahwa dokumen yang telah dinotarisasi secara digital memiliki kekuatan hukum yang sama seperti dokumen yang telah ditandatangani oleh notaris konvensional. Kekuatan hukum dari dokumen yang telah dinotarisasi secara digital mungkin bisa saja berbeda tergantung dari yurisdiksi pengguna jasa.

Tanda persetujuan pengguna jasa *Genuinedoc* untuk memanfaatkan *Genuinedoc* ialah dari (1) mendaftarkan aplikasi pendaftaran kepada genuine.com atau (2) menggunakan layanan notarisasi *genuinedoc*.

B. *Pretty Good Privacy*[38]

Pretty Good Privacy (PGP) adalah program komputer yang menyediakan kriptografi rahasia (*cryptographic privacy*) dan otentikasi. PGP dikembangkan oleh Paul Zimmerman sejak 1991 dan terus berkembang hingga saat ini oleh Zimmerman maupun lainnya.

PGP cukup berpengaruh dalam dunia komputer dan protokol operasi maupun data formatnya telah distandarisasikan untuk dapat beroperasi antar PGP dari versi yang berbeda maupun dari *software* yang berbeda. Pada saat ini, desain PGP diadopsi untuk menjadi standar dalam penelusuran jejak di dunia Internet, spesifikasi ini dikenal dengan nama OpenPGP.

PGP dapat mensandikan (*encrypt*) isi dari suatu data (file berkode biner maupun pesan teks), PGP sering dipakai untuk *e-mail* dan faksimili melalui internet, yang mana fasilitas tersebut tidak dilengkapi dengan keamanan data. Pada mulanya PGP digunakan untuk *e-mail* dengan cara mensandikan pesan ke dalam format khusus (bahasa

---

[38] Lihat situs, <http://www.pgp.com>, diakses tanggal 14 Juli 2006.

American Standard Code for Information Interchange/ASCII armor) untuk mencegah perubahan isi ketika sedang dikirimkan.

PGP berjalan dengan cara menggunakan kriptografi kunci publik (*public-key cryptography*) dan kriptografi kunci simetris (*symmetric key cryptography*), dan termasuk sistem yang membatasi kunci publik ke identitas pengguna. Edisi pertama dari sistem ini dikenal luas dengan nama web of trust dan terus digunakan sampai saat ini. Versi terbaru PGP sudah termasuk Infrastuktur Kunci Publik (*Public Key Infrastructure*/PKI).

PGP menggunakan kunci algoritma enkripsi kunci asimetris (*asymmetric key encryption*). Dalam hal ini, penerima harus memiliki pasangan kunci, yakni sebuah kunci publik dan kunci rahasia. Pengirim menggunakan kunci publik penerima untuk mensandikan kunci rahasia untuk sebuah algoritma *symmetric cipher*. Kunci tersebut dipergunakan untuk mensandikan pesan teks. Banyak pengguna kunci publik PGP dapat memperoleh kunci tersebut pada komputer server kunci PGP yang bertindak sebagai *mirror sites* terhadap satu dan lainnya.

Penerima dari pesan yang terproteksi oleh PGP mengubah penyandian menggunakan *session key* untuk sebuah algoritma simetris. *Session key* tersebut tentunya ada dalam pesan namun dalam bentuk terenkripsi dan di dekripsi menggunakan kunci rahasia dari si penerima.

Apabila digunakan secara benar, PGP merupakan sarana yang memiliki tingkat keamanan yang sangat tinggi. Hanya NSA (*National Security Agency*/Badan Keamanan Nasional Amerika Serikat) yang dapat membuka *cryptography* tersebut. Hingga ahli *cryptography* Bruce Schneier berpendapat bahwa PGP merupakan bentuk *cryptography* mendekati enkripsi level militer.

Dalam Syarat dan Ketentuan Penggunaan PGP (*Term and Conditions of Use*) dijelaskan bahwa dengan menggunakan situs PGP, menandakan bahwa pengguna jasa telah setuju untuk terikat kepada aturan penggunaan PGP.

PGP juga berkomitmen untuk menghargai Hak Atas Kekayaan Intelektual (HaKI) penggunanya, maka dari itu PGP memberikan sanksi tegas apabila ada pengguna yang melanggar HaKI atas pengguna lainnya berupa penghentian account atau hak akses pengguna yang melanggar. Apabila ada dugaan pelanggaran HaKI, maka PGP memberikan prosedur pelaporan dugaan tersebut dengan cara:

1. Surat kuasa fisik maupun elektronik yang ditujukan kepada orang yang ditunjuk untuk mewakili kepentingan pemilik hak cipta;
2. Deskripsi dari hasil karya yang telah di hak ciptakan yang diduga dilanggar hak ciptanya;
3. Deskripsi atas lokasi suatu isi yang melanggar hak cipta dalam situs PGP;
4. Alamat, nomor telepon dan alamat *e-mail* sehingga PGP dapat menghubungi pengguna jasa;
5. Pernyataan yang menerangkan bahwa pengguna jasa memiliki itikad baik bahwa pelanggaran tersebut bukan karena persetujuan pemilik hak cipta, agennya, atau karena hukum;
6. Pernyataan bahwa pengguna jasa menyatakan bahwa pengguna jasa jujur mengenai pemberitahuan yang ditujukan kepada PGP dan pengguna jasa adalah pemegang hak cipta atau kuasa yang bertindak atas nama pemegang hak cipta.

C. *Verisign*[39]

Perusahaan ini didirikan sejak 1995, sebagai anak perusahaan hasil *spin-off* dari perusahaan *RSA Security* yang bergerak dalam bidang sertifikasi keamanan. Perusahaan baru ini memperoleh lisensi dalam bidang kunci kriptografi yang telah dipatenkan RSA dan perjanjian untuk tidak bersaing untuk waktu yang terbatas. Perusahaan ini melayani sebagai CA (*Certificate Authority*) yang masih dijalani hingga saat ini. Motto perusahaan ketika diluncurkan ialah "*providing trust for the Internet and Electronic Commerce through our Digital Authentication services and products.*" (menyediakan kepercayaan untuk Internet dan Perdagangan Elektronik melalui pelayanan dan produk otentikasi digital).

Verisign sekarang melayani tiga juta sertifikasi, dari bidang militer sampai jasa keuangan dan perusahaan retail aplikasi, *Verisign* menjadi CA terbesar dalam masalah enkripsi dan otentikasi di internet.

Untuk menggunakan produk dan jasa *Verisign*, maka akan dimintakan informasi tentang pengguna, tergantung tipe produk dan jasa yang diinginkan. Informasi yang diminta berupa nama, alamat, nomor telepon, alamat *e-mail*, nomor kartu kredit, nomor rekening

[39] Lihat situs, <http://www.verisign.com/verisign-inc/index.html>, diakses tanggal 14 Juli 2006.

bank, alamat IP (*Internet Protocol/IP Address*), dan atau nomor jaminan sosial (*social security number*).

Verisign bekerjasama dengan sumber database pihak ketiga dalam rangka lebih menjamin otentikasi identitas dan atribut lain mengenai pengguna. Hal ini juga untuk mencegah pencurian identitas.

Verisign diwajibkan oleh hukum untuk membuka informasi kepada pemerintah lokal, negara bagian, federal, nasional maupun internasional (sebagai contoh membuka informasi tentang pembeli produk *software* kepada Departemen Perdagangan Amerika Serikat, Biro Administrasi Ekspor, seperti yang diwajibkan dalam perjanjian ekspor). *Verisign* juga akan membuka informasi kepada pihak ketiga dalam rangka penegakan hukum dan peraturan perundangan. *Verisign* juga akan membagi informasi terkait dengan penyelidikan, pencegahan atau mengambil tindakan terhadap aktifitas ilegal atau dugaan pemalsuan.

Verisign dalam menghadapi dugaan pelanggaran HaKI membuat prosedur pelaporan secara tertulis kepada mereka dengan syarat:

1. Pernyataan bahwa pelapor adalah pemegang hak cipta yang memiliki hak ekslusif dan hak tersebut telah dilanggar, atau sebuah pernyataan bahwa pelapor memiliki kewenangan untuk bertindak berdasarkan kuasa dari pemegang kuasa dimana terdapat dugaan pelanggaran
2. Sebuah pernyataan, dengan menyatakan sebenar-benarnya bahwa informasi yang diberikan adalah akurat.
3. Identifikasi dari materi yang di klaim telah terjadi pelanggaran dan informasi secukupnya untuk memberitahu *Verisign* mengenai keberadaan materi tersebut.
4. Informasi secukupnya mengenai hak *Verisign* menghubungi pelapor, termasuk alamat, nomor telepon, nomor fax, dan *e-mail*.
5. Pernyatan bahwa pelaporan tersebut berlandaskan itikad baik dan penggunaan material tersebut tidak berdasarkan ijin dari pemegang hak cipta, maupun karena hukum.

D. *i-trust*[40]

Dalam suatu proses transaksi yang menggunakan media elektronik, informasi dari pihak-pihak yang bertransaksi harus dapat

---

[40] Lihat situs, <http://www.plasa.com/informasi/b2b/i-trust.php>, diakses tanggal 20 Juli 2006.

dijamin bebrapa aspek yang meliputi keamanan, otentikasi, otorisasi serta integritasnya. Aspek-aspek tersebut merupakan suatu landasan bagi terciptanya suatu iklim transaksi melalui media elektronik (*e-commerce*) yang baik.

Layanan yang menyediakan sertifikasi elektronik (*Certificate Authority*) untuk memfasilitasi sistem keamanan transaksi informasi secara komprehensif, meliputi layanan digital signature dan *public key encryption.*

Telkom's Public Key Infrastructure (Telkom's PKi): Suatu kemampuan yang menyeluruh untuk menyediakan public key encryption dan digital signature.

Public Key Infrastructure berfungsi untuk memfasilitasi *digital signature* sebagai *Public Key* dan pengacakannya atau enkripsi sebagai *Private Key.* Analogi dari kedua fungsi ini adalah seperti halnya penerbitan kartu ATM selalu terdiri dari sepasang kunci pertama adalah nomor kartu atau *Public Key* yang bisa diberikan kepada publik yang kedua adalah nomor PIN (*Private Key*) yang hanya diketahui oleh si pemegang kartu saja.

V. Tanggung Jawab Rahasia Jabatan

Seperti yang telah disebutkan dalam A.2., bahwa notaris sebelum menjalankan jabatannya wajib mengucapkan sumpah/janji menurut agamanya dihapadan menteri atau pejabat yang ditunjuk.

Substansi Sumpah/janji yang berkenaan dengan tanggung jawab rahasia jabatan ialah "...Bahwa saya akan merahasiakan isi akta dan keterangan yang diperoleh dalam pelaksanaan jabatan saya..." Apabila ditafsirkan secara gramatikal berarti notaris wajib memegang teguh rahasia apapun yang berkaitan dengan isi dan atau apapun yang ia ketahui berkaitan dengan akta dan informasi-informasi terkait lainnya.

Berdasarkan hal tersebut, bukan berarti notaris akan selalu menyimpan rahasia. Notaris tetap bisa membuka rahasia selama hal ini diwajibkan oleh hukum (asas legalitas). Sebab notaris bersumpah berjanji bahwa

> *... patuh dan setia kepada Negara Republik Indonesia, Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang tentang Jabatan Notaris serta peraturan perundang-undangan lainnya ...*
>
> *... bahwa saya akan menjaga sikap, tingkah laku saya, dan akan menjalankan kewajiban saya sesuai dengan kode etik profesi, kehormatan, martabat, dan tanggung jawab ...*

Sehingga prinsip akuntabilitas dan keterbukaan yang dijalankan oleh notaris tetap harus berpegang teguh pada peraturan perundang-undangan dan kode etik notaris. Apabila diminta oleh Pengadilan maupun hukum yang berlaku maka notaris harus membuka rahasia yang terkait dengan suatu permasalahan.

Notaris juga harus memperhatikan jadwal retensi arsip. Jadwal retensi arsip ialah daftar yang berisi tentang jangka waktu penyimpanan arsip yang dipergunakan sebagai pedoman penyusutan arsip.

VI. Penutup

A. Simpulan

1. Penyelenggaraan jasa tanda tangan elektronik merupakan suatu bentuk penyelenggaraan sistem informasi elektronik untuk membantu identifikasi terhadap suatu individu secara *online*. Tanda tangan elektronik bukan dalam bentuk tanda tangan konvensional yang kemudian di migrasi ke dalam bentuk gambar digital (*digitized image*), bukan juga suatu tanda tangan yang ditulis diatas perangkat keras yang memiliki fasilitas layar sentuh (*touch screen*). Tanda tangan elektronik ialah hasil proses enkripsi suatu elektronik yang dilakukan matematis atau elektronik yang dikirimkan melalui perangkat keras yang terhubung dengan jaringan *cyberspace*. Hal ini dilakukan dengan maksud mengidentifikasi pesan yang dikirimkan, memastikan bahwa pesan yang dimaksud bukan dikirim oleh orang lain. Tanda tangan elektronik juga dijalankan untuk tujuan tertentu, yaitu cerminan dari suatu tindakan persetujuan (*approval*). Tanda tangan elektronik juga memproteksi isi/substansi dokumen dan arsip dari tindakan-tindakan perubahan isi/substansi.
2. Dalam perspektif hukum kearsipan dan dokumentasi perusahaan, dokumen memiliki tingkatan tergantung dari substansi dan siapa yang menandatangani dokumen tersebut. Dokumen yang dimaksud ialah:
    1) dokumen keuangan yang terdiri dari catatan, bukti pembukuan, dan data pendukung administrasi keuangan, yang merupakan bukti adanya hak dan kewajiban serta kegiatan usaha suatu perusahaan.
    2) Dokumen lainnya terdiri dari data atau setiap tulisan yang berisi keterangan yang mempunyai nilai guna bagi

perusahaan meskipun tidak terkait langsung dengan dokumen keuangan.

3. Sedangkan arsip ialah:

   1) naskah-naskah yang dibuat dan diterima oleh Lembaga-lembaga Negara dan Badan-badan Pemerintahan dalam bentuk corak apapun, baik dalam keadaan tunggal maupun berkelompok, dalam rangka pelaksanaan kegiatan pemerintah;
   2) naskah-naskah yang dibuat dan diterima oleh Badan-badan Swasta dan/ atau perorangan, dalam bentuk corak apapun, baik dalam keadaan tunggal maupun berkelompok, dalam rangka pelaksanaan kehidupan kebangsaan.

      Apabila dokumen dan arsip tersebut di migrasi ke dalam bentuk digital dengan cara yang baik dan benar sesuai dengan prinsip-prinsip yang diatur dalam *electronic record management* menjadi *E-doc*, maka tidak mengurangi keabsahan dan otentik dari dokumen yang dimaksud.

   3) Sebelum memanfaatkan jasa tanda tangan elektronik, antara penyelenggara dan pengguna telah meyepakati syarat dan ketentuan termasuk di dalamnya klausula baku yang telah ditetapkan oleh penyelenggara. Dimana apabila dipahami substansinya selalu menguntungkan penyelenggara jasa. Pedoman penyelenggaraan jasa harus dipahami oleh pengguna, sebab ketidak cermatan pengguna dalam memahami isi perjanjian dapat menimbulkan kerugian bagi pengguna.

B. Saran

Penyelenggaraan tanda tangan elektronik dan dokumentasi digital merupakan suatu bentuk kebutuhan yang keberadaannya dapat hidup berdampingan dengan penyelenggaraan tanda tangan dan dokumentasi konvensional. Masing-masing dapat saling menutupi kelebihan maupun kekurangan satu dan lainnya.

Perkembangan pengaturan hukum terhadap Penyelenggaraan tanda tangan elektronik dan dokumentasi digital harus tetap dinamis. Sebab, perkembangan teknologi yang kian pesat apabila tidak di antisipasi dan diikuti dengan serangkaian kebijakan dan regulasi pemerintah, maka negara kita cepat atau lambat tertinggal dengan

negara-negara lain yang lebih antisipatif menghadapi perkembangan hukum telematika.

Sejalan dengan hal ini, praktek perdagangan global sudah hampir tidak mengenal batas. Sehingga pemanfaatan jasa yang mendukung perdagangan dimaksud akan terus dibutuhkan demi mencapai kondisi yang lebih kompetitif.

DAFTAR PUSTAKA

Buku

Black, Henry Campbell., *Black's Law Dictionary.* Minnesota: West Publishing. 1991.

Badrulzaman, Mariam., Mencari Sistem Hukum Benda Nasional, Cet. II. Bandung: Alumni. 1997.

Burns, James Mac Gregor, J.W. Peltason, dan Thomas E. Crowin., Ed. *Government by The People.* New Jersey: Prentice Hall, 1989.

Burch, John G., *Information System: Theory and Practice.* California: Hamilton Publishing Company, 1974.

Friedman, Lawrence M., *American Law an Introduction*, 2nd. Ed. New York: W.W. Norton and Co. 1998.

Harahap, M. Yahya., Hukum Acara Perdata, Jakarta: Sinar Grafika, 2005.

Holmes, Douglas., *E-Business Strategy for Government.* First Edition. London: Nicholas Brearly Publishing, 2001.

Indrajit, Richardus Eko., *Electronic Government*: Strategi Pembangunan Pengembangan Sistem Pelayanan Publik Berbasis Teknologi Digital. Yogyakarta: Andi, 2002.

Lubis, Suhrawardi K., Etika Profesi Hukum, Jakarta: Sinar Grafika, 1994.

Lundgren, Terry D. *Records Management In The Computer Age.* Massachusetts: PWS-KENT. 1989.

Mason, Stephen., *Electronic Signature.* Singapore: LexisNexis, 2003.

Mann, Ronald J. Dan Winn, Jane K., *Electronic Commerce.* New York: Aspen Law and Business, 2002.

Mertokusumo, Sudikno., Mengenal Hukum: Suatu Pengantar, Yogyakarta: Liberty, 1999.

Nasution, Az., Hukum Perlindungan Konsumen Suatu Pengantar. cet. 2. Jakarta: Diadit Media, 2002.

Nico., Tanggung Jawab Notaris selaku Pejabat Umum. Yogyakarta: CDSBL, 2003

Notodisuryo, R. Sugondo., Hukum Notariat di Indonesia, Jakarta: Raja Grafindo Persada, 1993.

Osborne, David dan Peter Plastrick., *Banishing Bureaucracy: The Five Strategies for Reinventing Government*. New York: Addison Wesley Publishing Company, 1997.

Prodjodikoro, Wirjono., Azas-asas Hukum Perdata, Cet. I. Bandung: Sumur, 1959.

Sembiring, M.U., Tehnik Pembuatan Akta, Medan: Program Pendidikan Spesialis Notariat Fakultas Hukum Universitas Sumatra Utara, 1997.

Soebekti, R., Aneka Perjanjian, Cet.IX. Bandung: Citra Aditya Bakti, 1995.

_____, Hukum Perjanjian, Cet.XVI. Jakarta: Intermasa, 1996.

_____, Pokok-pokok Hukum Perdata, Cet.XXV. Jakarta: Intermasa, 1993.

Samsul, Inosentius. Perlindungan Konsumen Kemungkinan Penerapan Tanggung Jawab Mutlak. Jakarta: FHUI Pascasarjana, 2004.

Soekanto, Soerjono., Pengantar Penelitian Hukum, Cet.III. Jakarta: UI-PRESS, 1986.

Soeprapto, Maria Farida Indrati., Ilmu Perundang-Undangan, Cet. 11. Jakarta: Kanisius, 1998.

Sofwan, Sri Soedewi Masjchoen., Hukum Perdata: Hukum Benda, Cet.V. Yogyakarta: Liberty, 2000.

Tan, Thong Kie., Studi Notariat Beberapa Mata Pelajaran dan Serba-serbi Praktek Notaris, Jakarta: Ichtiar Baru Van Houve, 2000.

Tobing, G.H.S. Lumban., Peraturan Jabatan Notaris, Jakarta: Erlangga, 1996.

Peraturan Perundang-Undangan

Indonesia, *Undang-Undang Tentang Jabatan Notaris*. UU No. 30. LN No. 117 Tahun 2004..

_____, *Undang-Undang Tentang Ketentuan-Ketentuan PokokKekuasaan Kehakiman. UU No. 14. LN No. 74 Tahun 1970 TLN No. 2951.*

_____, *Undang-Undang Tentang Perubahan Atas Undang-Undang Nomor 14 Tahun 1970 Tentang Ketentuan-Ketentuan Pokok Kekuasaan Kehakiman. UU No. 35. LN No. 147 Tahun 1999 TLN No. 3879.*

_____, *Undang-Undang Tentang Dokumen Perusahaan, UU No. 8. LN No. 18 Tahun 1997 TLN No. 3674.*

_____, *Rancangan Undang-Undang Republik Indonesia Tentang Informasi dan Transaksi Elektronik.*

_____, *Instruksi Presiden tentang Kebijakan dan Strategi Nasional Pengembangan E-Government. Inpres No. 3 Tahun 2003, Lembaran Lepas 2003*

_____, *Instruksi Presiden Republik Indonesia tentang Pusat Informasi Berbasis Teknologi Informatika di Komplek Kemayoran. Inpres No. 1 Tahun 2001.*

_____, *Tata Cara Pengalihan Dokumen Perusahaan Ke Dalam Mikrofilm Atau Media Lainnya Dan Legalisasi. PP No. 88. LN No. 195 Tahun 1999 TLN No. 3913.*

Departemen Komunikasi dan Infromasi, Keputusan Menteri Hukum dan Perundang-undangan Republik Indonesia tentang Sistem Administrasi Badan Hukum. Kepmen No. M.01.HT.01.01 Tahun 2000.

_____, *Keputusan Menteri Komunikasi dan Informasi Tentang Panduan Manajemen Sistem Dokumen Elektronik. Kepmen No. 56/KEP/M.KOMINFO/12/2003.*

_____, *Keputusan Menteri Komunikasi Dan Informasi Nomor: 56/KEP/M.KOMINFO/12/2003 Tentang Panduan Manajemen Sistem Dokumentasi Elektronik.*

Majalah dan Koran

"*Investasi Asing Turun 40%, PMDN Naik 78%*", Bisnis Indonesia 16 Juni 2004.

_____, "*Swasta Agar Dilibatkan Percepat CAP* (*Community Access Point*)", 15 Juni 2004.

_____, "*Setahun Inpres E-Government: Pertarungan Kekuasaan dan Akses Informasi Publik*", 15 Juni 2004.

_____, "*Cyberlaw di Indonesia Sulit Diwujudkan*", 26 Mei 2004.

_____, "*Raja Amazon Jeff Bezos*", 23 November 2005.

Internet

"An Overview Of "Open Source" Projects and License", <http://www.abanet.org/intelprop/opensource.html>, diakses tanggal 20 Juli 2006.

American Bar Association Section of Science and Technology Information Security System, *"Digital Signature Guidelines Tutorial"*, <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>, diakses tanggal 3 Juli 2006.

"Pentingnya Hukum di Jagat Maya Internet", <http://www.kontan-online.com/04/43/refleksi/ref2.htm>, diakses tanggal 2 Desember 2005.

Juni, Sabaruddin., *"Aspek Hukum Perdata Pada Perlindungan Konsumen"*, <http://www.library.usu.ac.id/download/fh/perdata-sabaruddin3.pdf>, diakses tanggal 14 Juli 2006.

"Kebijakan Makro Teknologi." <http://www.nakertrans.go.id/Info%20Telematika/makalah%20dan%20artikel/kebijakan%makro%20ti.htm>, diakses tanggal 2 Desember 2005.

Magfirah, Esther Dwi., *"Perlindungan Konsumen Dalam E-Commerce"*, <http://www.solusihukum.com/artikel/artikel31.php>, diakses tanggal 14 Juli 2006.

Priharnowo, Thoso., *"Mahkamah Konstitusi Tolak Keberagaman OrganisasiNotaris"*, <http://www.tempointeraktif.com/hg/hukum/2005/09/13/brk,20050913-66523,id.html>, diakses tanggal 25 Nopember 2005.

Setiyadi, Mas Wirgantoro Roes., *"E-Government Sebagai Suatu Investasi: Mengukur Resiko Keuntungan dan Kegagalan-Keberhasilan Implementasi E-Government di Pemerintah Daerah"*, <http://www.gipi.or.id/page.php/halamandepan/artikel>, diakses tanggal 2 Desember 2005.

<http://www.plasa.com/informasi/b2b/i-trust.php>, diakses tanggal 20 Juli 2006.

<http://www.verisign.com/verisign-inc/index.html>, diakses tanggal 14 Juli 2006.

<http://www.pgp.com/>, diakses tanggal 14 Juli 2006.

<www.tecrime.com/0gloss.htm>, diakses tanggal 14 Juli 2006.

<http://www.genuinedoc.com/index.html>, diakses tanggal 14 Juli 2006.

<http://www.uncitral.org/pdf/english/workinggroups/wg_ec/wp-80.pdf>, diakses tanggal 3 Juli 2006.

<http://www.azleg.state.az.us/ars/41/00351.htm>, diakses tanggal 3 Juli 2006.

<http://www.ftc.gov/os/2001/06/esign7.htm>, diakses pada tanggal 3 Juli 2006.

<http://www.mycert.org.my/bill.html>, diakses tanggal 3 Juli 2006.

<http://www.bakernet.com/ecommerce/singapore-t.htm>, diakses pada tanggal 3 Juli 2006.

<http://en.wikipedia.org/wiki/Public_key_infrastructure>, diakses tanggal 20 Juli 2006.

<http://en.wikipedia.org/wiki/Certificate_authority>, diakses pada tanggal 20 Juli 2006.

Santoso, Wicaksono Wahyu., "*Keberadaan RUU Tanda Tangan Digital Dan Transaksi Elektronik Kaitannya dengan Kesiapan Masyarakat Pelaku Usaha dan Sistem Penegakan Hukum*", Ikhtnet 31 Juli 2004, <http://Ikht.net/artikel_lengkap.php?id= 14>, diakses tanggal 3 Juli 2006.