ELECTRONIC SIGNATURE DI SINGAPURA

Suci Lestari, S.H., M.H.*

Abstrak

Penelitian ini menggunakan metode yuridis normatif untuk melihat sejauh mana *electronic signature* diatur dalam peraturan yang berlaku, baik dalam hukum positif yang ada di Singapura maupun pada hukum yang berlaku internasional. Metode analisis yang digunakan dalam penulisan ini yaitu deskriptif analitis yang sifat pemaparan yang bertujuan untuk memperoleh gambaran mengenai pengaturan *electronic signature* dalam transaksi elektronik. Hasil penelitian yang ditemukan adalah bahwa *electronic signature* memiliki kegunaan yang besar dalam memberikan pengamanan terhadap pertukaran informasi elektronik dalam *e-commerce*. Karena memiliki peranan yang besar dalam perdagangan dan sifatnya yang *border-less*, *electronic signature* dalam *e-commerce* juga diatur oleh aturan-aturan hukum internasional seperti UNCITRAL *Model Law on Electronic Commerce*, UNCITRAL *Model Law on Electronic Signature*, *The General EU Electronic Commerce Directive* – 4 Mei 2000, *Electronic Signature Directive* - 30 November 1999, *Brussels Convention on Online Transactions* - 1 Maret 2002 dan GUIDEC *(General Usage for International Digitally Electronic Commerc*e). Lebih lanjut ditemukan bahwa penggunaan *electronic signature* dalam suatu transaksi elektronik memiliki fungsi yang sama dengan tanda tangan konvensional, sehingga diakui keabsahannya dalam hukum pembuktian. Sedangkan dalam peraturan hukum positif di Singapura, *electronic signature* diatur dalam *Electronic Transactions Act*. Meskipun demikian, *electronic signature* masih perlu diatur lebih lanjut dan disosialisasikan kepada masyarakat.

Kata Kunci : *Electronic Signature*, Tanda Tangan Elektronik, *Digital Signature*, Tangan Tangan Digital

---

* Dosen Biasa pada Fakultas Hukum Universitas Trisakti
E-mail : suci_law@yahoo.com

This research using juridical normative method of to see the extent to which electronic signature arranged in regulations, either in positive law in Singapore as well as on international law. A method of analysis used in this research is descriptive analytical which exposure to descriptive the aims to obtain an idea of setting electronic signature in electronic transaction. The research found is that electronic signature having usefulness that is great in giving security to exchange information electronic in e-commerce. Because it has a large role in trade and border-less, electronic signature in e-commerce also governed by such rules of international law as in UNCITRAL Model Law on Electronic Commerce, UNCITRAL Model Law on Electronic Signature, The General EU Electronic Commerce Directive – 4th May 2000, Electronic Signature Directive – 30th November 1999, Brussels Convention on Online Transactions – 1st March 2002 and GUIDEC (General Usage for International Digitally Electronic Commerce). Further it was found that the use of electronic signatures within an electronic transaction has the same functionality as conventional signatures, so that its validity is recognized in the law of proof. Whereas in positive legislation in Singapore, electronic signature provided for in the Electronic Transactions Act. Nevertheless, the electronic signature will still need to set up further and socialized to the public.

Keyword : Electronic Signature, Digital Signature

PENDAHULUAN

I. Latar Belakang

Republik Singapura adalah sebuah negara kota di lepas ujung Selatan Semenanjung Malaya, 137 kilometer (85 mil) di Utara Khatulistiwa di Asia Tenggara. Perekonomiannya sangat bergantung pada ekspor dan pengolahan barang impor. Singapura memiliki salah satu pelabuhan tersibuk di dunia dan merupakan pusat pertukaran mata uang asing terbesar keempat di dunia setelah London, New York dan Tokyo. Ekonomi Singapura termasuk di antara sepuluh negara paling terbuka, kompetitif dan inovatif di dunia dan dianggap sebagai negara paling ramah bisnis di dunia[1].

Arus globalisasi ekonomi telah membawa pengaruh yang signifikan bagi pertumbuhan dan perkembangan dunia usaha, termasuk perkembangan bisnis di Singapura. Karenanya, Singapura harus bereaksi dengan cepat dan tangkas dalam membuat undang-undang dan institusi-institusi baru, atau menyesuaikan undang-undang dan institusi-institusi yang sudah ada. Dalam hal ini, Singapura telah siap dan bersedia belajar dari perkembangan-perkembangan hukum yang terjadi di luar negeri, jika memiliki kesamaan aspirasi. Kadang-kadang, cara-cara penyelesaian masalah yang sudah kuno harus diganti dengan ide-ide baru yang telah teruji dengan modifikasi-modifikasi yang tepat agar sesuai dengan keadaan setempat. Dengan perdagangan dan investasi sebagai denyut nadi utama ekonomi Singapura, maka sistem hukum Singapura harus secara berkelanjutan memberikan perlindungan yang memadai kepada semua pihak dan memberi inspirasi kepercayaan dalam komunitas bisnis internasional [2].

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 difahami oleh pihak yang tidak berhak *(Privacy/Confidentiality);* identitas pihak yang terkait dapat diketahui atau dijamin otentisitasnya *(Authentication);* informasi yang dikirim dan diterima tidak berubah *(Integrity);* dan pihak yang terkait tidak dapat menyangkal telah melakukan transaksi *(Non- Repudiation)*[3].

Pengamanan terhadap informasi (pesan) yang dikirim dalam suatu transaksi melalui media elektronik menempati tataran paling tinggi dan sangat penting. Fakta menunjukkan perubahan pesan-pesan elektronik dapat dilakukan dengan mudah dan

---

[1] http://id.wikipedia.org/wiki/Singapura diunduh tanggal 20 Oktober 2011 pukul 22.46 WIB

[2] http://www.singaporelaw.sg/content/LegalSystIndon.html diunduh tanggal 20 Oktober 2011 pukul 23.03 WIB

[3] Kebutuhan dasar dari *e-contract* antara lain adalah sebagai berikut:

1. Identifikasi yang jelas dari para pihak yang akan melakukan kontrak;
2. Identifikasi yang jelas terhadap subyek utama kontrak;
3. Identifikasi yang jelas dari batas waktu yang dituangkan dalam kontrak;
4. Tanda tangan yang valid dari para pihak, yang disertai dengan tanggal pembuatan kontrak.
5. Kontrak yang ditandatangani tidak dapat diubah oleh siapapun dan tidak ada yang bisa mengingkarinya (*non-repudiation*).

tidak terdeteksi, sehingga meningkatkan risiko terjadinya manipulasi terhadap pesan elektronik yang dikirim. Meningkatnya penggunaan jaringan komunikasi terbuka *(internet)* akan meningkatkan pula risiko 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 risiko tersebut termasuk penggunaan infrastruktur kunci publik. Dewasa ini, kebutuhan akan kerahasiaan informasi serta penjagaan atas keaslian suatu informasi dirasa semakin meningkat. Pembentukan *framework* untuk otentikasi dari informasi berbasis komputer memerlukan pengetahuan dan ketrampilan akan hukum dan bidang keamanan komputer. Akan tetapi, mengkombinasikan antara kedua hal ini bukan pekerjaan yang mudah. Konsep yang ada di dunia hukum seringkali hanya berkorelasi sedikit dengan konsep yang ada pada dunia keamanan komputer. Sebagai contoh, konsep "tanda tangan elektronik" (*electronic signature*) yang dikenal pada dunia keamanan komputer adalah hasil dari penerapan teknik-teknik komputer pada suatu informasi. Sedangkan di dunia umum, tanda tangan mempunyai arti yang lebih luas, yaitu tanda atau lambang nama yang yang dibuat dengan maksud untuk melegalisasi dokumen yang ditandatangani. Tanda tangan elektronik merupakan suatu cara untuk menjamin keaslian suatu dokumen elektronik dan menjaga supaya pengirim dokumen dalam suatu waktu tidak dapat menyangkal bahwa dirinya telah mengirimkan dokumen tersebut. Tanda tangan elektronik menggunakan algoritma-algoritma serta teknik-teknik komputer khusus dalam penerapannya.

Penelitian ini akan menitikberatkan pada analisis yuridis *electronic signature* di Singapura. Dipilihnya Singapura sebagai negara tempat fokus penelitian karena negara ini telah menerapkan *electronic signature* dalam berbagai bidang dan memiliki *Electronic Transactions Act* yang berlaku mulai tanggal 10 Juli 1998 dan diubah terakhir pada tahun 2011 serta merupakan negara pelopor *electronic signature* model *hybrid* di *The Third Wave* (Generasi Ketiga).

II. Tujuan Penelitian

1. Mengetahui bagaimana konsep pengaturan *electronic signature* di Singapura.
2. Mengetahui bagaimana kesesuaian pengaturan *electronic signature* di Singapura dengan *UNCITRAL's Uniform Rules on Electronic Signatures*.

III. Perumusan Masalah

1. Bagaimana konsep pengaturan *electronic signature* di Singapura ?
2. Bagaimana kesesuaian pengaturan *electronic signature* di Singapura dengan *UNCITRAL's Uniform Rules on Electronic Signatures* ?

IV. Pertanyaan Penelitian

1. Bagaimana konsep pengaturan *electronic signature* di Singapura ?
2. Bagaimana kesesuaian pengaturan *electronic signature* di Singapura dengan *UNCITRAL's Uniform Rules on Electronic Signatures* ?

KAJIAN PUSTAKA

A. PENGERTIAN *ELECTRONIC SIGNATURE*

1. Istilah *Electronic Signature* dan *Digital Signature*

Dalam Pasal 2 *UNCITRAL Model Law on Electronic Signatures (with Guide to Enactment 2001)* diatur definisi tandatangan elektronik[4] adalah data dalam bentuk elektronik yang berkaitan atau secara logikal berhubungan dengan pesan data, yang dapat digunakan untuk mengidentifikasi si pemilik tanda tangan yang berkaitan dengan pesan data dan sebagai tanda persetujuan pemilik tanda tangan atas informasi yang terdapat di dalam pesan data tesebut.

Bentuk tandatangan elektronik antara lain : *password*, nama yang diketik di akhir email (*a typed name at the end of an e-mail*), *personal identification number* (PIN), tombol saya setuju (*I-Agree buttons*), indikator biometrik dan tandatangan digital (*digital signature*). Dari segala jenis tandatangan elektronik maka tandatangan digital (*digital signature*) adalah yang secara luas digunakan sebagai acuan.

Istilah *digital signature* seringkali rancu dengan istilah *electronic signature*, walaupun di atas ditunjukkan bahwa *electronic signature* adalah istilah umum teknologi dalam kaitannya terhadap teknologi yang memenuhi ketentuan perundang-undangan, dimana *digital signature* menggunakan teknologi yang spesifik. *Digital Signature* dibentuk dan diverifikasi menggunakan kriptografi.

2. Bentuk *Electronic Signature*

Istilah *electronic signature* dipergunakan untuk menegaskan konsep generic dari tanda tangan yang dibuat meggunakan komputer atau sarana mirip komputer[5]. Berbagai bentuk *electronic signature*, antara lain :

a. *Typing a name into an electronic document*[6] (mengetik nama dalam dokumen elektronik)
b. *'Click wrap' method of indicating agreement*[7] (metode *'Click wrap'* untuk menunjukkan persetujuan)
c. *Personal identification number (PIN)*[8]
d. *The name in an e-mail address* (nama dalam alamat surat elektronik)[9]

---

[4] *Article 2. Definitions (a) "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.*

[5] http://www.stephenmason.eu/e-signatures/ diunduh tanggal 15 April 2012 pukul 14.59 WIB

[6] http://www.stephenmason.eu/e-signatures/typing-a-name-in-an-electronic-document/ diunduh tanggal 15 April 2012 pukul 15.05 WIB

[7] http://www.stephenmason.eu/e-signatures/click-wrap/ diunduh tanggal 15 April 2012 pukul 15.06 WIB

[8] http://www.stephenmason.eu/e-signatures/pin/ diunduh tanggal 15 April 2012 pukul 15.07 WIB

[9] http://www.stephenmason.eu/e-signatures/name-in-e-mail-address/ diunduh tanggal 15 April 2012 pukul 15.08 WIB

e. *A manuscript signature that has been scanned*[10] (manuskrip tanda tangan yang dipindai)
f. *The digital biodynamic version of a manuscript signature*[11] (versi digital biodinamik dari tandatangan manuskrip)
g. *The digital signature*[12] (tandatangan digital)

3. Tujuan Tanda Tangan

Secara umum, penandatanganan suatu dokumen bertujuan untuk memenuhi keempat unsur di bawah ini[13] :

a. Bukti: Sebuah tanda tangan mengotentikasikan suatu dokumen dengan mengidentifikasikan penandatangan dengan dokumen yang ditandatangani.
b. Formalitas: Penandatanganan suatu dokumen 'memaksa' pihak yang menandatangani untuk mengakui pentingnya dokumen tersebut.
c. Persetujuan: Dalam beberapa kondisi yang disebutkan dalam hukum, sebuah tanda tangan menyatakan persetujuan pihak yang menandatangani terhadap isi dari dokumen yang ditandatangani.
d. Efisiensi: Sebuah tanda tangan pada dokumen tertulis sering menyatakan klarifikasi pada suatu transaksi dan menghindari akibat-akibat yang tersirat di luar apa yang telah dituliskan.

Kebutuhan-kebutuhan formal dari suatu transaksi legal, termasuk kebutuhan akan tanda tangan, berbeda-beda dalam setiap sistem hukum legal dan rentang waktu tertentu. Meskipun hal-hal alamiah mengenai suatu transaksi tidak berubah, hukum hanya memulai untuk mengadaptasi terhadap teknologi mutakhir.

4. Atribut Tanda Tangan

Untuk mencapai tujuan dari penandatanganan suatu dokumen seperti di atas, sebuah tanda tangan harus mempunyai atribut-atribut berikut :

1. Otentikasi penandatangan : sebuah tanda tangan seharusnya dapat mengindentifikasikan siapa yang menandatangani dokumen tersebut dan susah untuk ditiru orang lain.
2. Otentikasi dokumen : sebuah tanda tangan seharusnya mengidentifikasikan apa yang ditandatangani, membuatnya tidak mungkin dipalsukan ataupun diubah (baik dokumen yang ditandatangani maupun tandatangannya) tanpa diketahui.

Otentikasi penandatangan dan dokumen adalah alat untuk menghindari pemalsuan dan merupakan suatu penerapan konsep "*non-repudiation*" dalam bidang keamanan informasi. *Non-repudiation* adalah jaminan dari keaslian ataupun penyampaian dokumen asal untuk menghindari penyangkalan dari penandatangan

---

[10] http://www.stephenmason.eu/e-signatures/scanned-manuscript-signature/ diunduh tanggal 15 April 2012 pukul 15.09 WIB

[11] http://www.stephenmason.eu/e-signatures/biodynamic-signature/ diunduh tanggal 15 April 2012 pukul 15.11 WIB

[12] http://www.stephenmason.eu/e-signatures/digital-signature/ diunduh tanggal 15 April 2012 pukul 15.12 WIB

[13] http://www.informatika.org/~rinaldi/Kriptografi/Makalah/Makalah12.pdf diunduh tanggal 20 Oktober 2011 pukul 23.40 WIB

dokumen (bahwa dia tidak menandatangani dokumen tersebut) serta penyangkalan dari pengirim dokumen (bahwa dia tidak mengirimkan dokumen tersebut).

5. Kelemahan Dan Keunggulan *Electronic Signature*

Kelemahan yang masih menyertai teknologi tanda tangan elektronik adalah :

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

Sedangkan kelebihan yang paling utama dari adanya tanda tangan elektronik adalah lebih terjaminnya otentikasi dari sebuah dokumen. Tanda tangan elektronik sangat sulit dipalsukan dan berasosiasi dengan kombinasi dokumen dan kunci privat secara unik.

B. CARA KERJA TEKNOLOGI *ELECTRONIC SIGNATURE*

Tanda tangan elektronik dibuat dengan menggunakan teknik kriptografi, suatu cabang dari matematika terapan yang menangani tentang pengubahan suatu informasi menjadi bentuk lain yang tidak dapat dimengerti dan dikembalikan seperti semula. Kriptografi, sebagai batu bata utama untuk keamanan *e-commerce* adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman[14]. Di dalam kriptografi dikenal berbagai macam istilah misalnya *cryptanalysis* yaitu ilmu pengetahuan yang mempelajari bagaimana mengetahui *(compromise/defeat)* mekanisme kriptografi. *Cryptology* berasal dari bahasa Yunani, *krypto* dan *logos* yang berarti *hidden world* adalah suatu bidang yang mengkombinasikan *Cryptography* dan *Cryptoanalysis*[15].

Penggunaan istilah aman dalam kriptografi adalah relatif, sehingga kriteria aman yang dipergunakan disini adalah :

1. *Confidentiality* (kerahasiaan); suatu pesan tidak boleh dapat dibaca atau diketahui oleh orang yang tidak berkepentingan.
2. *Authenticity* (otentisitas); penerima pesan harus mengetahui atau mempunyai kepastian siapa pengirim pesan dan bahwa benar pesan itu dikirim oleh pengirim. Istilah ini juga berhubungan dengan suatu proses verifikasi terhadap identitas seseorang.
3. *Integrity* (integritas/keutuhan); penerima harus merasa yakin bahwa pesan yang diterimanya tidak pernah diubah sejak pesan itu dikirim hingga diterima,

---

[14] Direktorat Jenderal Perdagangan Dalam Negeri, Departemen Perindustrian dan Perdagangan bekerja sama dengan Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT-FHUI), Naskah Akademik Rancangan Undang_Undang Tentang Tanda Tangan Elektronik Dan Transaksi Elektronik (Depok,2001),hal.17. lihat di *http://www.bogor.net/idkf/onno/raw-data/digital-review-of-asia-pacific/manuscript/3.08-regulatory-environment/dprin.go.id/ruu-tte.pdf*

[15] Muhammad Aulia Adnan, "Aspek Hukum Protokol Pembayaran Visa/Mastercard *Secure Electronic Transaction* (SET)", Skripsi, Fakultas Hukum Universitas Indonesia, Depok, Jawa Barat, 2001, hal.23. mengutip Bruce Schneir, *Applied Crypthography*, 2nd ed.,(NewYork : John Willey and Sons Inc., 1996) hal.2. tersedia di *www.geocities.com/amwibowo/resource/**hukum**/**hukum**_set.pdf*

seorang pengacau tidak dapat mengubah atau menukar isi pesan yang asli dengan yang palsu.

4. *Non repudiation* (tidak dapat disangkal); pengirim pesan tidak dapat menyangkal bahwa ia tidak pernah mengirim pesan tersebut.

Penggunaan kriptografi dalam *e-commerce* (internet) telah banyak membantu dalam menyelesaikan masalah keamanan (*security*) dan juga masalah hukum. Kriptografi memungkinkan terciptanya suatu sistem komputer yang terpercaya (*trustworthy computer system*)[16].

Tanda tangan elektronik digital *public key cryptography* (kriptografi kunci publik), dimana algoritmanya menggunakan dua buah kunci, yang pertama adalah kunci untuk membentuk tanda tangan elektronik atau mengubah data ke bentuk lain yang tidak dapat dimengerti, dan kunci kedua digunakan untuk verifikasi tanda tangan elektronik ataupun mengembalikan pesan ke bentuk semula. Konsep ini juga dikenal sebagai *assymmetric cryptosystem* (sistem kriptografi non simetris).

Sistem kriptografi ini menggunakan kunci privat, yang hanya diketahui oleh penandatangan dan digunakan untuk membentuk tanda tangan digital, serta kunci publik, yang digunakan untuk verifikasi tanda tangan digital. Jika beberapa orang ingin memverifikasi suatu tanda tangan digital yang dikeluarkan oleh seseorang, maka kunci publik tersebut harus disebarkan ke orang-orang tersebut. Kunci privat dan kunci publik ini sesungguhnya secara matematis 'berhubungan' (memenuhi persamaan-persamaan dan kaidah-kaidah tertentu). Walaupun demikian, kunci privat tidak dapat ditemukan menggunakan informasi yang didapat dari kunci publik.

Proses lain yang tak kalah penting adalah fungsi *hash*, digunakan untuk membentuk sekaligus memverifikasi tanda tangan elektronik. Fungsi hash adalah sebuah algoritma yang membentuk representasi digital atau semacam "sidik jari" dalam bentuk nilai *hash* (*hash value*) dan biasanya jauh lebih kecil dari dokumen aslinya dan unik hanya berlaku untuk dokumen tersebut. Perubahan sekecil apapun pada suatu dokumen akan mengakibatkan perubahan pada "nilai hash" yang berkorelasi dengan dokumen tersebut. Fungsi hash yang demikian disebut juga "fungsi hash satu arah", karena suatu nilai hash tidak dapat digunakan untuk membentuk kembali dokumen aslinya. Oleh karenanya, fungsi hash dapat digunakan untuk membentuk tanda tangan elektronik. Fungsi hash ini akan menghasilkan "sidik jari" dari suatu dokumen (sehingga unik hanya berlaku untuk dokumen tersebut) yang ukurannya jauh lebih kecil daripada dokumen aslinya serta dapat mendeteksi apabila dokumen tersebut telah diubah dari bentuk aslinya.

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

1. Pembentukan tanda tangan elektronik menggunakan nilai *hash* yang dihasilkan dari dokumen serta kunci privat yang telah didefinisikan sebelumnya. Untuk menjamin keamanan nilai *hash* maka seharusnya terdapat kemungkinan yang sangat kecil bahwa tanda tangan elektronik yang sama dapat dihasilkan dari dua dokumen serta kunci privat yang berbeda.
2. Verifikasi tanda tangan elektronik adalah proses pengecekan tanda tangan elektronik dengan mereferensikan ke dokumen asli dan kunci publik yang telah

[16] *Ibid.*

diberikan, dengan cara demikian dapat ditentukan apakah tanda tangan elektronik dibuat untuk dokumen yang sama menggunakan kunci privat yang berkorespondensi dengan kunci publik.

Untuk menandatangani sebuah dokumen atau informasi lain, penandatangan pertama-tama membatasi secara tepat bagian-bagian mana yang akan ditandatangani. Informasi yang dibatasi tersebut dinamakan "*message*". Kemudian aplikasi tanda tangan elektronik akan membentuk nilai hash menjadi tanda tangan elektronik menggunakan kunci privat. Tanda tangan elektronik yang terbentuk adalah unik baik untuk *message* dan juga kunci privat.

Umumnya, sebuah tanda tangan elektronik disertakan pada dokumennya dan juga disimpan dengan dokumen tersebut juga. Bagaimanapun, tanda tangan elektronik juga dapat dikirim maupun disimpan sebagai dokumen terpisah, sepanjang masih dapat diasosiasikan dengan dokumennya. Karena tanda tangan elektronik bersifat unik pada dokumennya, maka pemisahan tanda tangan elektronik seperti itu merupakan hal yang tidak perlu dilakukan.

Proses pembentukan dan verifikasi tanda tangan elektronik 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 tangan elektronik akan dapat menghubungkan/mengasosiasikan dokumen dengan penandatangan. Tanda tangan elektronik tidak dapat dipalsukan, kecuali penandatangan kehilangan kontrol dari kunci privat miliknya.
2. Otentikasi Dokumen : Tanda tangan elektronik 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 elektronik 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 elektronik menyediakan tingkat kepastian yang tinggi bahwa tanda tangan yang ada merupakan tanda tangan sah dan asli dari pemilik kunci privat. Dengan tanda tangan elektronik, 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.

Sifat yang diinginkan dari tanda tangan elektronik diantaranya adalah :

a. Tanda tangan asli (otentik), tidak mudah ditulis/ ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti sehingga penandatangan tidak bisa menyangkal bahwa dulu ia tidak pernah menandatanganinya,

b. Tanda tangan itu hanya sah untuk dokumen (pesan) itu saja. Tanda tangan itu tidak bisa dipindahkan dari suatu dokumen ke dokumen lainnya . Ini juga berarti bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak sah lagi.

c. Tanda tangan itu dapat diperiksa dengan mudah.
d. Tanda tangan itu dapat diperiksa oleh pihak-pihak yang belum pernah bertemu

dengan penandatangan.

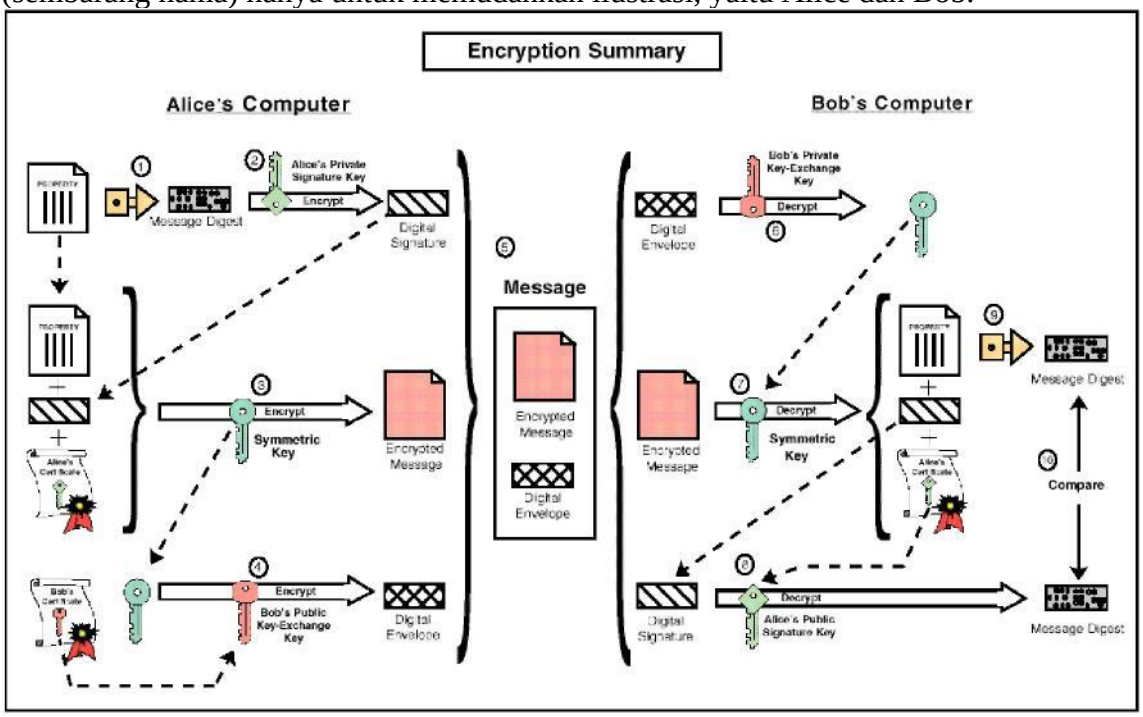
e. Tanda tangan itu juga sah untuk kopi dari dokumen yang sama persis[17].

C. *ELECTRONIC SIGNATURES* DALAM TRANSAKSI ELEKTRONIK

Transaksi Elektronik Dengan Kriptografi

Penggunaan kriptografi atau *public-key algorithm* dalam menandatangani suatu dokumen akan menimbulkan kerumitan-kerumitan. Dibawah ini akan diterangkan dalam bentuk ringkasan (*summary*) tentang proses tandatangan elektronik.

Untuk memudahkan penjelasan maka akan digunakan dua buah nama (sembarang nama) hanya untuk memudahkan ilustrasi, yaitu Alice dan Bob.



RANGKUMAN DARI PENGGUNAAN KRIPTOGRAFI

Gambar diatas menunjukan proses kriptografi yang terjadi dalam *digital signature*. Langkah-langkah dalam melakukan enkripsi ini adalah sebagai berikut :

No/langkah	Penjelasan
1	Alice menjalankan (*runs*) data yang hendak ia kirimkan, melalui algoritma satu arah (*one way algorithm*) sehingga ia mendapat satu 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 *message digest*

[17] Direktorat Jenderal Perdagangan Dalam Negeri, Departemen Perindustrian dan Perdagangan bekerja sama dengan Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT-FHUI),*op.cit.*, hal 22-23.

	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 mengunakan kunci itu melakukan enkripsi terhadap data yang hendak ia kirimkan , tandatangani (*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 (kopi) dari kunci publik milik Bob. Untuk menjamin keamanan transmisi dari kunci simetris maka kunci 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 sertifikat digital, serta kunci simetris yang telah dienkripsi dengan kunci asimetris (*digital envelope*).
6	Bob menerima pesan (*message*) dari Alice tersebut dan kemudian mendekripsi amplop digital dengan kunci privat 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 mengunakan kunci privat milik Alice. Kalau hasil dari perbandingan itu adalah tidak sama maka data tersebut pastilah telah diubah atau dipalsukan setelah ditandatangani.

Ringkasan mengenai cara komunikasi aman dengan kiptografi kunci publik[18]

[18] *Ibid*., hal.27-28.

D. STANDAR PENGAKUAN *ELECTRONIC SIGNATURES* DAN SKIM LISENSINYA

1. Latar Belakang[19]

Sebuah infrastruktur kunci publik (*public key infrastructure* / PKI) yang umumnya disediakan oleh *Certification Authority* (CA), memilik standar pengoperasian proses sertifikat yang dikenal dengan istilah *certification practice statement* (CPS). Sayangnya, CPS dari sebuah CA ke CA lainnya bisa berbeda-beda.

Artinya, seorang *relying party* bisa saja tidak mempunyai tanda tangan atau sertifikat digital seorang *subscriber* dari sebuah CA lain yang memilik CPS yang berbeda dengan CPS yang telah biasa diakui sang *relying party*.

Dengan kata lain, dua orang yang berasal dari domain CA yang berbeda, bisa jadi saling tidak mengakui tanda tangan yang dihasilkan dari domain lainnya dengan alasan bahwa standar CPS dari kedua CA tersebut berbeda.

Yang menarik adalah, bisa saja kedua CA tersebut menganggap CPS miliknya masing-masing lebih tinggi kualitasnya dibandingkan yang lain. Sebenarnya dalam pembahasan teknis mengenai PKI, sudah dijelaskan mengenai bagaimana cara CA bisa mengakui keberadaan CA lainnya. Ini dapat dilakukan antara lain dengan *cross certification*, *hierarchial networktree*, dan lain sebagainya.

Sebenarnya ada cara non-teknis (lebih konseptual) agar tanda tangan yang berasal dari dua domain dapat diakui. Hal ini dilakukan dengan cara menetapkan suatu standar operasi minimal yang harus dipatuhi CA. Dengan memenuhi standar operasi minimal, maka sertifikat digital ataupun tanda tangan elektronik yang dihasilkan dari sebuah *domain* CA tertentu dapat diakui pihak manapun yang telah mengakui standar operasi minimal tersebut. Contoh spesifiknya, dalam hal mengelola sertifikat, maka CA tersebut harus tunduk pada standar CPS minimal.

Patut diperhatikan bahwa pihak yang mengakui standar operasi tersebut tidak hanya *relying party* dalam pengertian sempit, namun pihak seperti negara (terutama peradilan di negara tersebut) juga dapat mengakui standar tersebut, terlepas dari yang membuat standar minimal itu pemerintah itu sendiri atau bukan.

Dalam bab ini kita tidak membicarakan secara teknis apa yang harus termaktub dalam standar minimum tersebut, melainkan lebih kearah bagaimana standar itu diakui oleh banyak pihak (termasuk oleh pemerintah).

Di beberapa negara, seperti yang akan dijelaskan nanti, pemerintah memberikan lisensi kepada CA yang sudah beroperasi pada standar minimum tertentu.

Pembahasan pada bab ini juga akan sangat penting untuk pembahasan pada hukum internasional, karena berurusan dengan cara bagaimana mengakui keberadaan tanda tangan elektronik yang dihasilkan dari negara lain yang mungkin memilik standar operasi CA yang berbeda.

Ada berbagai cara untuk mengakui keberadaan suatu tanda tangan. Maksudnya, tidak peduli apakah ada *cross-certification* atau tidak antar *domain* CA, yang penting adalah standar operasi CA-CA tesebut tunduk kepada batasan minimal yang diakui negara. Artinya, setiap warga negara dalam juridiksi negara tersebut harus mengakui tanda-tangan digital yang diakui oleh negara.

2. Tingkat Standar Pengakuan[20]

---

[19] *Ibid.*, hal. 132.
[20] *Ibid.*, hal. 133.

Menurut Chris Kuner dkk.[21], ada beberapa cara jenis standar pengakuan terhadap tanda tangan elektronik yang diakui negara, termasuk, yaitu mengenakan standar minimalistik (longgar), mengenakan standar ketat,atau penerapan beberapa standar.

a. Standar Minimalistik (longgar)[22]

Pelaksanaan tanda tangan elektronik memiliki kemungkinan terjadi kekurang-otentik-an yang dilatarbelakangi oleh buruknya pengoperasian CA. Sebagaimana diatur dalam Pasal 14 UU ITE yang menyatakan bahwa penyelenggara sertifikasi elektronik (CA) harus menyediakan informasi mengenai metode yang digunakan untuk mengidentifikasi penanda tangan, hal yang dapat digunakan untuk mengetahui data diri pembuat tanda tangan elektroni, dan hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan tanda tangan elektronik. Uraian ini menunjukkan adanya sifat diversitas metode, pengidentifikasi tanda tangan, dan keberlakuan serta keamanan. Sehingga kemungkinan, perbedaan pedoman CA yang satu dengan CA yang lain sangat mungkin terjadi.

Keamanan tanda tangan elektronik yang menggunakan sistem kriptografi kunci publik memang lebih terjaga dibandingkan dengan penggunaan sistem operasi kriptografi kunci simetris. Namun, jika dibandingkan dengan sistem tanda tangan konvensional maka tanda tangan elektronik lebih dipertimbangkan keamanan terlepas dari adanya potensi pemalsuan terhadap tanda tangan elektronik, karena nantinya pemalsuan tersebut sudah masuk ke dalam domain tindak pidana komputer. Namun, pengadilan, misalnya, dengan berlakunya rezim UU ITE tidak tidak boleh menolak pembuktian melalui tanda tangan elektronik.

Beberapa negara *common law* (misalnya Kanada, Australia, dan Amerika Serikat) mengakui tanda tangan elektronik di pengadilan, terlepas apakah telah memenuhi standar baku atau belum. Negara-negara tersebut menerapkan sistem kebelakuan minimalistik, yakni tidak secara ketat hanya menerima pembuktian tanda tangan elektronik yang memenuhi standar baku.

b. Penerapan Standar Ketat[23]

Di sisi lain, ada pula pula negara-negara yang sistem peradilanya hanya menerima tanda tangan elektronik yang sudah dijamin dahulu “keamanannya “.

Artinya tanda tangan elektronik yang dihasilkan oleh suatu CA tersebut harus sulit sekali dipalsukan, sehingga negara berani menjamin keotentikanya. Pada umumnya, penerapan standar ketat Ini dilakukan dengan cara mewajibkan audit terhadap CA oleh auditor yang dapat dipercaya, berkenaan dengan standar operasi dan CPS-nya .setelah menerima hasil audit yang menyatakan bahwa sistem operasi dan CPS dari CA tersebut dianggap cukup layak dan aman, negara dapat memberikan lisensi[24].

---

[21] *An Analysis of International Electronic and Digital Signature Implementation Initiatives , A Study Prepared for the Internet Law & Policy Forum* (ILPF), September, 2000 lihat di http://www.ilpf.org/groups/analysis_IEDSII.htm diunduh pada tanggal 28 Juli 2012 pukul 23.19 WIB

[22] Direktorat Jenderal Perdagangan Dalam Negeri, Departemen Perindustrian dan Perdagangan bekerja sama dengan Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT-FHUI),*op.cit.,* hal 134.

[23] *Ibid.*, hal. 134-135.

[24] Istilah lain untuk CA berlisensi adalah *designated* CA (CA yang telah ditunjuk) atau r*ecognized* CA (CA yang telah diakui) kepada CA.

Tanda tangan elektronik yang di hasilkan oleh infrastruktur kunci publik CA berlisensi tersebut dapat langsung diakui pengadilan tanpa perlu dibuktikan dahulu (*presumption of authenticity*).

c. Penerapan Beberapa Standar atau Dua Standar[25]

Tetapi ada juga negara-negara yang mengakui keberadaan tanda tangan elektronik, baik yang berasal CA yang berlisensi dengan CA yang tidak berlisensi. Jadi kalau ada skema lisensi CA pun, tidak berarti bahwa semua CA wajib berlisensi. Singapura memiliki skim lisensi CA yang tidak wajib.

Namun jika dibandingkan CA yang tidak berlisensi, maka CA yang berlisensi memiliki beberapa keuntungan yang tidak dimiliki CA yang tidak berlisensi.

Keuntungan tersebut antara lain:

1) Prinsip pembuktian terbalik atas keaslian tanda tangan elektronik di pengadilan. Tanda tangan elektronik yang dihasilkan dari PKI CA berlisensi tersebut langsung diakui dipengadilan sederajat dengan tanda tangan biasa. Jadi jika ingin dibantah, maka harus dibuktikan sebaliknya (bahwa CA tersebut melanggar standar operasi yang ditetapkan untuk mendapatkan lisensi).
2) Adanya *reliance limit* jika CA harus memberikan ganti rugi terhadap *subscriber*-nya manakala terjadi bencana / masalah.
3) Adanya pemberian jaminan kepada pihak ketiga (*relying party*) dari negara dan sebagainya.

Sedangkan untuk tanda tanda tangan elektronik yang berasal dari CA yang tidak berlisensi, saat persidangan harus dibuktikan dahulu bahwa sistem PKI (termasuk standar operasi dan CPS-nya) dari CA yang bersangkutan sudah cukup aman (*secure*). Namun menurut pendapat penulis, pembuktian dengan cara ini amat rentan karena amat mudah dibantah. Selain Singapura, Hong Kong juga memiliki skim lisensi yang tidak wajib.

3. Cara Penetapan Standar Pengakuan[26]

Penulis berpendapat ada beberapa cara bagaimana pengadilan suatu negara dapat mengakui tanda tangan elektronik :

a. Masyarakat yang menetapkan standar pengakuan (*customary law*)

Andaikan tidak ada standar baku yang diakui resmi oleh pemerintah (tidak semua negara bagian di Amerika menerapkan memiliki standar resmi), mungkin kita bertanya, bagaimanakah suatu tanda tangan elektronik dapat diakui keberadaannya ?

Seperti kita ketahui, dalam sistem *common law*, suatu keputusan dalam peradilan terdahulu menjadi hukum bagi keputusan peradilan di masa depan. Dugaan penulis, bisa saja suatu standar tidak ditetapkan oleh negara, tapi ditetapkan oleh peradilan dan masyarakat. Sebagai contoh, misalnya peradilan, dan masyarakat mengakui hasil audit oleh sebuah auditor swasta terhadap sebuah CA. Bisa saja hasil audit dari auditor swasta itu diakui oleh pengadilan, yang berimplikasi tanda tangan digital yang dihasilkan dari CA tersebut memiliki kekuatan sama dengan tanda tangan biasa.

b. Pemerintah / negara menetapkan standar baku dan memberikan lisensi kepada CAs

Untuk menghasilkan tanda tangan yang ”aman” (*secure*), maka standar operasi CA tersebut harus diaudit oleh negara. Pada umumnya, auditing ini berkaitan dengan

---

[25] *Ibid.*, hal. 135-136.
[26] *Ibid.*, hal. 136-137.

skim lisensi terhadap CA. Jadi dapat disimpulkan di sini, bahwa negara menjamin keotentikan tanda tangan elektronik yang dihasilkan dari CA yang sudah berlisensi. Italia dan Argentina bahkan hanya mengakui tanda tangan elektronik dari CA yang berlisensi. Di sisi ekstrim, Malaysia melarang pendirian CA tanpa lisensi dari pemerintah.

Australia tidak memiliki standar baku untuk CA non-pemerintah, namun Australia memiliki standar baku pengopersian CA yang diwajibkan kepada lembaga pemerintah yang operasikan CA. Untuk catatan tambahan, setiap negara bagian di Amerika Serikat tetap diizinkan untuk menetapkan suatu standar tersendiri asal tidak bertentangan dengan undang-undang pemerintahan federal[27].

Jika sebuah negara bagian memiliki standar sendiri, maka sebenarnya negara bagian tersebut menerapkan 2 standar yang saling melengkapi, yakni standar minimalistik dari pemerintah federal dan standar ketat dari pemerintah negara bagian.

4. Skim Pemberian Lisensi & Proses Audit[28]

Proses pemberian lisensi terhadap suatu CA merupakan masalah lain juga yang patut dicermati. Esensinya, sebenarnya, yang memberikan lisensi adalah 'pemerintah'. Sebelum mendapatkan lisensi, umumnya CA harus diaudit / diperiksa, apakah CA tersebut sudah bekerja sesuai standar tertentu atau belum. Standar lisensi tersebut umumnya standar tersebut ditentukan oleh negara. Meskipun standar tersebut bisa saja diadopsi dari perjanjian internasional, tetap saja pemerintahan dari setiap negara yang mengesahkan standar apa yang diakui negara. Ada beberapa macam cara bagaimana suatu skim lisensi dapat diberikan kepada sebuah CA :

a. Hanya ada sebuah badan pemerintah yang memberikan lisensi.
b. Bisa ada beberapa badan pemerintah yang memberikan lisensi, tergantung pada sektor mana CA itu berada.
c. Lembaga swadaya masyarakat yang diakui pemerintah yang terdiri dari pengguna, pelaku usaha, pemerintah, akademisi, pengacara dan lain-lain.

Mengenai cara melakukan audit ada beberapa cara :

a. Badan yang memberikan lisensi juga melakukan audid
b. Badan pemberi audit menunjuk auditor khusus untuk melakukan audit.

5. Analisis Sistem Standar pengakuan yang ada[29]

Dari pembahasan di atas nampak bahwa pada umumnya pada negara yang menerapkan pengakuan standar tanda tangan elektronik yang longgar, biasanya menggunakan mekanisme peradilan *common law* (meskipun tidak semua). Namun untuk negara-negara yang mengenakan standar tanda tangan elektronik yang ketat atau campuran, biasanya negara juga berperan dalam penentuan standar tersebut. Menurut pandangan kami, keuntungan dari sistem pengakuan standar longgar adalah :

---

[27] *One Hundred sixth Congres of the United States of America, Electronic in Signatures in Global and National Commerce Act (Washington: 2000).* lihat di http://www.gpo.gov/fdsys/pkg/BILLS-106s761enr/pdf/BILLS-106s761enr.pdf diunduh tanggal 29 Juli 2012 pukul 22.00 WIB

[28] Direktorat Jenderal Perdagangan Dalam Negeri, Departemen Perindustrian dan Perdagangan bekerja sama dengan Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT-FHUI),*op.cit.,* hal. 137-138.

[29] *Ibid.,* hal. 138.

a. Sangat efisien secara makro ekonomis, karena tidak perlu birokrasi yang berbelit-belit untuk menjadi CA.
b. Selain itu, ada dugaan bahwa kemungkinan sengketa terhadap keotentikan tanda tangan digital juga kecil. Jadi tidaklah perlu melakukan audit yang bertele-tele terhadap CA.

Sedangkan keuntungan dari system pemberlakuan standar pengakuan tanda tangan elektronik (dengan menggunakan CA berlisensi) yang ketat bagi masyarakat adalah :

a. Tingkat keamanan dari tanda tangan elektronik yang terjamin oleh negara
b. Kemungkinan manipulasi saat persidangan dapat diminimalisir (karena mengikuti standar baku)
c. Mendapatkan asumsi keaslian tanda tangan elektronik dipengadilan (*presumption of authencity*).

6. Penerapan Lisensi Untuk Trusted Third Party[30]

Jika kita melakukan generalisir, sebenarnya sebuah CA itu termasuk sebuah *trusted third party* (TTP), yang dalam bahasa Indonesia 'pihak ketiga'yang terpercaya'. Konsep yang cukup mirip - bahkan dapat dianggap sama dengan TTP - adalah konsep *trustworthy system* (sistem yang terpercaya).

Sekedar catatan , biasanya sistem sekuriti TTP yang ada saat ini menggunakan *kryptographi* kunci simetrik. Untuk memberikan gambaran, sistem kripthografi kunci simetrik sampai saat ini masih banyak sekali dipergunakan untuk bisnis, misalnya untuk transaksi keuangan / perbankan (baik yang retail maupun yang bernilai besar), pengaman transaksi EDI, komunikasi rahasia negara dan sebagainya.

Kalau kita perhatikan pembahasan –pembahasan sebelumnya, pengakuan negara (baik dengan standar minimalistik, standar ketat atau keduanya) adalah hanya terdapat tanda tangan elektronik (dengan kata lain, hanya terdapat sistem kriptografi kunci publik / PKI). Padahal, bisa saja PKI yang disediakan oleh sebuah CA tidak lebih aman dari TTP yang menggunakan
sistem kriptografi kunci simetrik .

Patut penulis tegaskan disini, bahwa memang benar secara umum kriptografi kunci publik (yang dipergunakan untuk tanda tangan digital) lebih aman ketimbang kriptografi kunci simetrik. Namun penting untuk diingat bahwa faktor implementasi juga sangat berpengaruh. Artinya, bisa saja kalau implementasi aplikasi PKI – nya ceroboh, sehingga akhirnya keamanannya menjadi lebih rendah ketimbang TTP yang menggunakan kriptografi kunci simetrik.

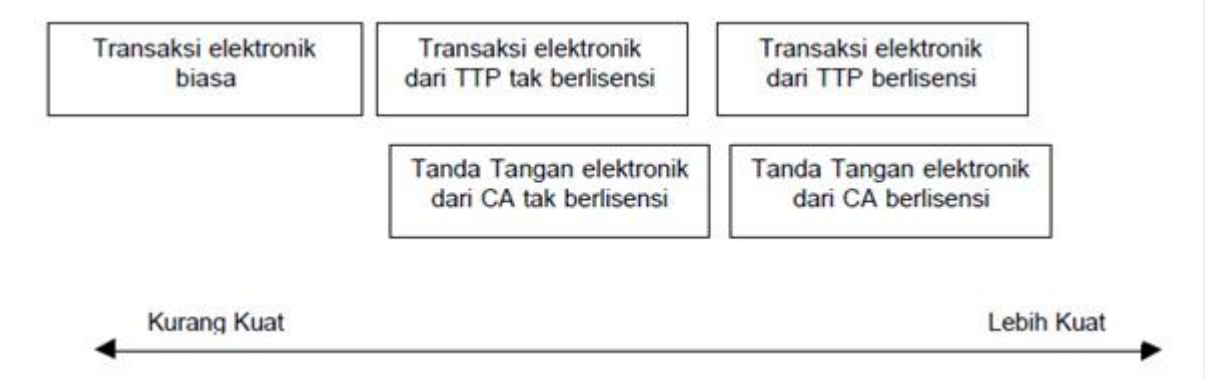
Ada beberapa hal yang kita bisa tarik dari konsep TTP, sehubungan dengan pengakuan keberadaaan hukum transaksi elektonik :

a. Jika benar sebuah kriptografi publik tidak pasti berarti lebih aman ketimbang TTP dengan kunci simetrik, maka seharusnya ada kesempatan bagi TTP dengan kunci simetrik untuk mendapatkan "lisensi" dari negara.
b. Jika ada TTP yang berlinsensi, dan skim lisensi itu tidak wajib, maka ada pula TTP yang tidak berlisensi.
c. Di luar semua itu, ada transaksi elektronik yang tidak melalui TTP apapun (transaksi elektronik biasa). Yang termasuk kategori ini mungkin file di disket

[30] *Ibid.,* hal. 138-140.

dan log transaksi tanpa pengamanan kriptografi atau teknik sekuriti digital lainnya.

Jika kita mengambil asumsi bahwa akan ada skim lisensi untuk TTP secara umum, maka menurut pandangan kami, pengakuan dan kekuatan hukum dari berbagai transaksi elektronik dan tanda tangan elektronik dapat digambarkan sebagai berikut.



Gambar. Kekuatan pembuktian transaksi elektronik dan tanda tangan elektronik secara hukum

Patut dicatat bahwa gambaran diatas hanya untuk memberikan gambaran umum saja. Banyak masalah yang kecil tapi mempengaruhi kuat-tidaknya suatu data elektronik. Satu hal lagi yang perlu diperhatikan dari gambar tersebut adalah kenyataan bahwa ada semacam "spektrum" kekuatan hukum dari data elektronik. Jadi memang, hukum itu tidak hitam-putih atau benar-salah, namun hanyalah kebenaran relatif.

METODE PENELITIAN

Untuk mencari dan menemukan jawaban dari rumusan permasalahan yang telah diajukan pada bab sebelumnya dalam penelitian ini, maka peneliti menggunakan prosedur dan teknik penelitian atau yang lebih dikenal dengan istilah metode penelitian. Pemilihan dan penggunaan prosedur dan teknik penelitian, bertujuan untuk dapat melakukan analisis terhadap data dan fakta yang telah diperoleh dengan disesuaikan pada tipe dan sifat dari penelitian yang bersangkutan. Dengan demikian, metode penelitian adalah suatu cara atau proses pemeriksaan atau penyelidikan yang menggunakan cara penalaran dan berpikir yang logis analitis (logika), berdasarkan dalil-dalil, rumusan dan teori-teori tertentu untuk mengadakan verifikasi serta menguji kebenaran dari suatu hipotesa tentang fenomena alamiah, fenomena sosial dan fenomena hukum tertentu[31].

Esensi dari metode penelitian dalam setiap penelitian hukum adalah mendeskripsikan mengenai tata cara atau teknik bagaimana suatu penelitian hukum tersebut dilakukan. Tata cara atau teknik tersebut biasanya mencakup uraian mengenai tipe atau metode penelitian, sifat penelitian, jenis data, alat pengumpulan data, analisis dan teknik pengambilan kesimpulan[32]. Pada dasarnya, penggunaan

---

[31] C.F.G. Sunaryati Hartono, *Penelitian Hukum Di Indonesia Pada Akhir Abad Ke-20* (Bandung : Alumni, 1994), hal.105.

[32] Bambang Waluyo, *Penelitian Hukum Dalam Praktek* (Jakarta : Sinar Grafika, 1996), hal.17-20.

metode dalam suatu kegiatan penelitian adalah bertujuan untuk dapat mempelajari satu atau beberapa fenomena dan menganalisanya berdasarkan fakta-fakta yang tersedia, yang kemudian akan memberikan suatu solusi terhadap masalah-masalah yang ditimbulkan oleh fakta tersebut[33].

Oleh karena itu, dalam penelitian hukum ini, maka peneliti akan menggunakan metode penelitian sebagai berikut :

1. Tipe Penelitian

Penelitian tentang "*Electronic Signature* Di Singapura" merupakan suatu penelitian hukum-normatif. Sebagai suatu penelitian hukum normatif, maka penelitian ini berbasis pada analisis norma hukum, dalam hal ini hukum dalam arti *law as it is written in the books* (dalam peraturan perundang-undangan). Alasan digunakannya tipe penelitian hukum normatif adalah bahwa penelitian ini menggunakan data sekunder yang diperoleh dengan cara melakukan studi dokumen. Pada penelitian hukum normatif, data sekunder merupakan sumber atau bahan informasi yang penting. Data sekunder tersebut dapat berbentuk buku-buku, hasil penelitian, peraturan perundang-undangan, kamus, bibliografi dan literaur-literatur lainnya yang bersifat siap pakai. Keseluruhan data sekunder tersebut dapat diklasifikasi kembali berdasarkan jenisnya ke dalam bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier[34].

Penelitian ini juga menggunakan metode penelitian hukum normatif yang melihat asas-asas hukum tentang tandatangan elektronik, khususnya mengenai *electronic signature* di Singapura dan UNCITRAL. Melalui metode ini, peneliti melakukan studi mengenai ketentuan normatif *electronic signature* di Singapura dan UNCITRAL.

Dipilihnya Singapura sebagai negara tempat fokus penelitian karena negara ini telah menerapkan *electronic signature* dalam berbagai bidang dan merupakan negara pelopor *electronic signature* model *hybrid* di *The Third Wave* (Generasi Ketiga) serta baru saja pada tahun 2011 merubah peraturannya. Singapura memiliki *Electronic Transactions Act* yang berlaku mulai tanggal 10 Juli 1998 dan diubah terakhir pada tahun 2011.

2. Data

Berdasarkan jenis dan bentuknya, data yang diperlukan dalam penelitian ini adalah data sekunder yang diperoleh melalui studi kepustakaan. Namun demikian, untuk melengkapi atau mendukung analisis data sekunder, tetap diperlukan wawancara dengan beberapa informan yang dinilai memahami beberapa konsep atau pemikiran yang ada dalam data sekunder, sejauh dalam batas-batas metode penelitian normatif.

Data kepustakaan digolongkan dalam tiga bahan hukum, yaitu bahan-bahan hukum primer, bahan-bahan hukum sekunder dan bahan-bahan hokum tersier. Bahan-bahan

---

[33] Soerjono Soekanto, *Pengantar Penelitian Hukum* ((Jakarta : UI Press, 1986*)*, hal.2.

[34]Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif : Suatu Tinjauan Singkat*, Cet-Kelima, (Jakarta : Raja Grafindo Persada, 2001), hal.13-14.

hukum primer meliputi produk lembaga legislatif.[35] Dalam hal ini, bahan yang dimaksud adalah Singapore's *Electronic Transactions Act* (*Chapter* 88) *revised edition* 2011[36]**,** *UNCITRAL Model Law on Electronic Signatures With Guide to Enactment* 2001, *UNCITRAL's Uniform Rules on Electronic Signatures,* Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik[37] serta peraturan-peraturan yang berkaitan. Bahan-bahan hukum sekunder yang terdiri dari buku-buku tentang hukum komputer atau hukum telematika, hukum, teknologi informasi, makalah hasil seminar, media cetak dan internet dan jurnal ilmiah. Bahan-bahan hukum tersier yang terdiri dari kamus hukum, kamus telematika. dan kamus teknik informatika.

Pengumpulan data dilakukan melalui studi kepustakaan. Studi kepustakaan dilakukan di beberapa tempat, seperti perpustakaan Fakultas Hukum dan Pascasarjana Hukum Universitas Indonesia, perpustakaan Fakultas Hukum Universitas Trisakti, *CJ Koh Law Library* di *National University of Singapore* maupun mengakses data melalui internet.

Data hasil penelitian ini dianalisis secara kualitatif, artinya data kepustakaan dan hasil wawancara dianalisis secara mendalam, holistik, dan komprehensif. Penggunaan metode analisis secara kualitatif didasarkan pada pertimbangan, yaitu pertama data yang dianalisis beragam, memiliki sifat dasar yang berbeda antara satu dengan lainnya, serta tidak mudah untuk dikuantitatifkan. Kedua, sifat dasar data yang dianalisis adalah menyeluruh (*comprehensive*) dan merupakan satu kesatuan bulat (*holistic*). Hal ini ditandai dengan keaneka ragaman datanya serta memerlukan informasi yang mendalam (*indepth information*).[38]

3. **Metode Analisis Data**

Metode analisis yang peneliti gunakan adalah metode analisis deskriptif. Analisis untuk memberikan gambaran yang menyeluruh mengenai fakta dan pemasalahan yang berhubungan dengan objek penelitian kemudian dilakukan analisis. Data sekunder yang telah terkumpul kemudian dianalisa secara deskriptif. Hubungan antara teori yang didapat dalam studi kepustakaan kemudian akan dikaji dalam bentuk analisa yang kemudian dituangkan dalam bentuk tesis. Analisa data dengan menggunakan teknik analisis deskriptif yang bertujuan untuk mengumpulkan fakta disertai dengan penafsiran data, data yang diperoleh akan diolah secara kualitatif yang berasal dari studi kepustakaan dan dianalisa dengan menggunakan pendekatan yuridis normatif, untuk selanjutnya disajikan dalam bentuk deskriptif guna mendapatkan kesimpulan.

4. Cara Penarikan Kesimpulan

Hasil penelitian ini akan dianalisis dengan menggunakan metode deduktif, artinya adalah metode menarik kesimpulan yang bersifat khusus dari pernyataan-

---

[35]Enid Campbell, et. al., *Legal Research, Materials and Methods* (Sydney: The Law Book Company Limited, 1988), hal. 1.

[36] Edisi 2011, mulai berlaku tanggal 31 Desember 2011.

[37] Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, disahkan,diundangkan dan mulai berlaku tanggal 21 April 2008, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

[38]Chai Podhista, "Theoretical, Terminological, and Philosophical Issue in Qualitative Research", dalam Attig, et. al. *A Field Manual on Selected QualitativeResearch Methods* (Thailand: Institute for Population and Social Research, Mahidol University, 1991), hal. 7.

pernyataan yang sifatnya umum. Metode ini dilakukan dengan cara menganalisis pengertian atau konsep-konsep umum, antara lain mengenai konsep tentang *electronic signature* dan konsep *digital signature* dari aspek Hukum Telematika (*cyber law*). Adapun kajian terhadap konsep yang sifatnya umum tersebut akan dianalisis secara khusus dari *Electronic Transactions Act* beserta peraturan lainnya yang berkaitan.

PEMBAHASAN

A. ASPEK HUKUM PENGATURAN *ELECTRONIC SIGNATURE* DALAM REGULASI INTERNASIONAL

Perkembangan teknologi dan media-media baru yang dipergunakan dalam praktek perdagangan baik skala nasional, regional, maupun internasional membuat organisasi internasional memandang perlu pengakuan dan pengaturan mengenai hukum teknologi informasi, khususnya mengenai transaksi elektornik dan eksistensi tanda tangan elektronik sebagai organ penting dalam pelaksanaan transaksi elektronik.

Beberapa negara telah mengakui keabsahan tanda tangan digital *(digital signature)* dalam transaksi yang dilakukan elektronik. namun dengan perbedaan antara satu hukum nasional suatu negara dengan negara yang lainnya, maka dibutuhkan satu unifikasi hukum mengenai *digital signature* yang dapat mengharmonisasikan hukum. Unifikasi hukum merupakan suatu langkah penyeragaman hukum atau penyatuan suatu hukum untuk diperlakukan bagi seluruh bangsa di suatu wiiayah negara tertentu sebagai hukum nasional di negara-negara tersebut.

Fungsi dilakukan unifikasi hukum yaitu untuk melenyapkan keraguan terhadap jaminan kepastian dan perlindungan hukum, selain itu untuk melapangkan lintas hubungan internasional dalam bidang bisnis internasional[39]. *Digital signature* diatur dalam beberapa konvensi-konvensi internasional, beberapa diantaranya yaitu UNCITRAL Model Law On Electronic Commerce dan UNCITRAL Model Law on Electronic Signature, *United Nations Convention on Contracts for the International Sale of Goods* (UNCSIG), dan *General Usage For International Digitally Ensured Commerce* (GUIDEC). Regulasi yang dikeluarkan oleh ketiga badan internasional tersebut banyak dijadikan sebagai bahan rujukan dan diadopsi ke dalam cyberlaw berbagai negara.

Beberapa landasan yuridis internasional dan nasional dari pelaksanaan tanda tangan elektronik :

1. *United Nations Commission on International Trade Law* (UNCITRAL) *Model Law On Electronic Commerce (with Guide to Enactment 1996)* dan *Model Law on Electronic Signatures (with Guide to Enactment 2001)*

UNCITRAL sebagai salah satu organisasi internasional yang memiliki fokus dalam perkembangan teknologi informasi merupakan organisasi yang pertama kali membahas mengenai dampak penting teknologi informasi terhadap perniagaan elektronik. Hasil dari UNCITRAL berupa *Model law,* yang sifatnya tidak mengikat, namun menjadi acuan atau model bagi negara-negara untuk mengadopsinya atau

---

39 Perlindungan Kepentingan Bisnis Dan Unifikasi Hukum Perdata ***Lihat di*** ***http://hukumperdatainternasionalbisnis.wordpress.com/*** diunduh tanggal 30 Juli pukul 00.34 WIB

memberlakukannya dalam hukum nasional. Pada tanggal 16 Desember 1996 PBB kemudian mengeluarkan *UNCITRAL Model law on Electronic Commerce.*

Model law merupakan model hukum yang ditujukan untuk menawarkan model hukum kepada negara-negara yang sudah atau belum mempunyai peraturan mengenai materi ini. *Model law* ini bersifat bebas bagi negara untuk mengikuti atau tidak[40]. Diharapkan melalui *model law* ini negara-negara di dunia melalui kontruksi hukum nasionalnya dapat beradaptasi dengan transaksi elektronik yang terus berkembang.

UNCITRAL telah menjadi dasar dan kerangka untuk hukum *e-commerce* di banyak negara di dunia. *Model law* ini pertama kali dikeluarkan pada 1995 yang kemudian disetujui oleh Majelis Umum PBB dengan Resolusi 51/162 pada tanggal 16 Desember 1996. UNCITRAL *model law* merupakan landasan untuk mengatur otentikasi, perlengkapan, dan dampak pesan elektronik berbasis komputer dalam perdagangan. Pasal 5 kemudian diadopsikan oleh UNCITRAL sebagai amandemen di Juni 1998. *Model law* ini terdiri atas:

a. definisi kontrak elektronik dan memberikan pengaturan penerimaan dan kekuatan pembuktian dari bukti elektronik;
b. peraturan yang didasarkan pada prinsip non diskriminasi;
c. mengatur *e-commerce* secara spesifik untuk perundang-undangan nasional atau undang-undang lain yang dibuat oleh negara/negara bagian; dan
d. memberikan aturan yang pasti untuk transaksi berbasis elektronik.

Tanda tangan elektronik dalam *model law* ini secara diatur secara eksplisit dan diakui memiliki kekuatan hukum sama dengan tanda tangan tradisional. Teknologi tanda tangan elektronik ini dapat diperkenalkan sebagai teknologi yang cocok, tanpa harus mengubah undang-undang. Ketentuan-ketentuan Pasal 7 dalam model hukum berhubungan erat dengan praktik yang sedang berlangsung.

Pasal 7 *Uncitral Model Law On Electronic Commerce,* tanggal 16 Desember tahun 1996 menyatakan bahwa

> *"(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if :*
>
> *(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and*
>
> *(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement*."

---

[40] Ketentuan dalam *Model Law* sifatnya tidak mengikat, akan tetapi apabila telah diadopsi atau merupakan syarat dari perjanjian internasional sebelumnya maka dapat berlaku penuh. Dalam kasus unik ini, para negara kontrak lainnya dapat memaksa negara lain untuk mengikuti standart *model law* tersebut. *Model Law* dapat menjadi hukum kebiasaan internasional bila telah diadopsi oleh banyak negara yang berpengaruh secara ekonomi dan politik dikalangan internasional. Lihat di Direktorat Jenderal Perdagangan Dalam Negeri, Departemen Perindustrian dan Perdagangan bekerja sama dengan Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT-FHUI),*op.cit.*, hal. 145.

Pasal 7 *Uncitral Model Law On Electronic Commerce* menyatakan bahwa apabila terdapat peraturan yang membutuhkan tandatangan seseorang maka persyaratan tersebut dapat dipenuhi oleh suatu *messages* apabila :

a. Terdapat suatu metode yang dapat mengidentifikasikan seseorang dapat memberikan indikasi bahwa informasi yang terdapat dalam suatu data *messages* telah disetujui olehnya; dan
b. Metode tersebut dapat diandalkan atau dapat digunakan dalam membuat atau mengkomunikasikannya dalam berbagai situasi, termasuk berbagai perjanjian. Hal ini berarti tanda tangan digital sebagai metode akurat untuk mengidentifikasi pelaku tandatangan tersebut dapat digunakan sebagai tanda tangan seperti yang dimaksud dalam perjanjian-perjanjian tradisional.

Pasal 7 *Uncitral Model Law On Electronic Commerce* tahun 1996 tersebut dapat dijadikan sebagai dasar hukum dalam penggunaan tanda tangan digital, kerena Indonesia sudah meratifikasinya melalui Undang-Undang Nomor 7 Tahun 1994 Tentang Ratifikasi WTO (*World Trade Organization*).

Selanjutnya, Pada Pasal 11 ayat (1) Undang-Undang No 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dijelaskan bahwa tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:

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

Pasal tersebut memberikan pengakuan secara tegas bahwa meskipun hanya merupakan suatu kode, tanda tangan elektronik memiliki kedudukan yang sama dengan tanda tangan manual pada umumnya yang memiliki kekuatan hukum dan akibat hukum. Persyaratan sebagaimana dimaksud dalam pasal 11 merupakan persyaratan minimum yang harus dipenuhi dalam setiap tanda tangan elektronik. Ketentuan ini membuka kesempatan seluas-luasnya kepada siapa pun untuk mengembangkan metode, teknik, atau proses pembuatan tanda tangan elektronik.

Selain *The UNCTTRAL Model law on Electronic Commerce,* ada juga *The UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 (the "2001 Model Law")* diadopsi sebagai implementasi dari UNCITRAL *Model law on Electronic Commerce. Model law* 2001 ini disusun untuk membantu negara dalam mengharmonisasikan, memodernisasikan, dan menciptakan secara lebih efektif mengenai tanda tangan elektronik. *The UNCITRAL Model Law on Electronic Signatures of 2001* merupakan implementasi (adopsi) dari *UNCITRAL Model Law on Electronic Commerce.* Pasal 7 UNCITRAL *Model Law on Electronic Commerce* ditujukan agar terdapat pemenuhan dari fungsi tanda tangan di dunia elektronik yang dapat membantu negara dalam mengharmonisasikan, memodernisasikan, dan

menciptakan kerangka legislatif yang adil, untuk dapat menangani secara lebih efektif masalah tanda tangan elektronik.

Eksistensi *model law* ini pada akhirnya dapat menjadi dasar hukum dalam pelaksanaan tanda tangan elektronik, sehingga adanya perlakukan antidiskriminasi terhadap dokumentasi tertulis dengan informasi elektronik. Diharapkan pedoman dari *model law* ini dapat mendorong adanya legislasi nasional di negara-negara dunia yang menyadari pentingnya regulasi mengenai tanda tangan elektronik.

Model Law 2001 memperhatikan prinsip bahwa tidak adanya diskriminasi terhadap berbagai teknik yang mungkin dapat dipakai untuk berkomunikasi atau di simpan informasinya secara elektronik *(technology neutrality).*

Dalam Pasal 2 *UNCITRAL Model Law on Electronic Signatures (with Guide to Enactment 2001)* diatur definisi tandatangan elektronik[41] adalah data dalam bentuk elektronik yang berkaitan atau secara logikal berhubungan dengan pesan data, yang dapat digunakan untuk mengidentifikasi si pemilik tanda tangan yang berkaitan dengan pesan data dan sebagai tanda persetujuan pemilik tanda tangan atas informasi yang terdapat di dalam pesan data tesebut.

Dalam *Model Law* 2001, telah diatur mengenai pengakuan terhadap tanda tangan elektronik asing pada pasal 12[42]. Pada dasarnya *Model Law* 2001 tersebut menganjurkan agar tidak ada diskriminasi terhadap tanda tangan elektronik asing dan sertifikat digital asing. Beberapa butir penting adalah :

a. Tempat pembuatan/ penggunaan dari tanda tangan elektronik dan sertifikat digital harus tidak boleh dijadikan pertimbangan hukum sah atau tidaknya tanda tangan atau sertifikat tersebut. Justru yang penting menjadi pertimbangan hukum adalah masalah keamanan teknisnya (ayat l).

---

[41] http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

Article 2. Definitions (a) "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.

[42] *Article 12. Recognition of foreign certificates and electronic signatures*

1. *In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:*
   (a) To the geographic location where the certificate is issued or the electronic signature created or used; or
   (b) To the geographic location of the place of business of the issuer or signatory.
2. *A certificate issued outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate issued in [the enacting State] if it offers a substantially equivalent level of reliability.*
3. *An electronic signature created or used outside [the enacting State] shall have the same legal effect in [the enacting State] as an electronic signature created or used in [the enacting State] if it offers a substantially*
   equivalent level of reliability.
4. *In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards and to any other relevant factors.*
5. *Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.*

b. Kemudian, tanda tangan elektronik dan sertifikat digital asing harus bisa diakui di depan hukum lokal, asalkan tanda tangan dan sertifikat tersebut memiliki standar kehandalan yang secara substansial sudah memenuhi standar hukum lokal (ayat 2dan 3).

c. Untuk menentukan tingkat kehandalan, maka dipergunakan standar-standar rujukan Internasional (ayat 4). Pasal *model law* tersebut juga menyebutkan bahwa jika kedua pihak sepakat untuk menggunakan jenis tanda tangan dan sertifikat digital tersebut, maka kesepakatan itu harus dianggap mencukupi untuk melakukan *cross border recognition*, selama kesepakatan tidak melanggar peraturan lokal. Pada penjelasan pasal 12 tersebut, dijelaskan bahwa, 'tidak melanggar keharusan peraturan lokal' sebenarnya merujuk ada peraturan yang tetap mengharuskan pengunaan tanda tangan biasa pada jenis perjanjian tertentu (seperti akta kelahiran, surat nikah, surat tanah dan sebagainya). Disini terjadi semacam ambiguitas dalam pasal 12, karena ayat 2, 3 dan 4 menjelaskan bahwa ada suatu tingkat kehandalan tertentu sebagai syarat pengakuan. Sedangkan pada ayat 5, disebutkan bahwa pengakuan bisa dilakukan langsung antara pihak-pihak yang bertransaksi. Meskipun dijelaskan bahwa ayat 5 harus memperhatikan ayat-ayat 2, 3 dan 4, namun menurut penulis, ayat 5 sulit diterapkan, karena memperhatikan prasyarat ayat-ayat sebelumnya. Yang perlu dipahami dari ayat 5 adalah semangat untuk memudahkan *cross border recognition* terhadap tanda tangan elektronik dan sertifikat digital karena jika untuk melakukan pengakuan terhadap tanda tangan elektronik asing harus selalu melalui proses audit dan akreditasi berdasarkan lokal terlebih dahulu, maka hal itu akan menimbulkan ekonomi biaya tinggi. Solusi ideal untuk mencari titik imbang untuk pengakuan tanda tangan asing harus diformulasikan.

2. *European Union* (Uni Eropa)

Uni Eropa mengeluarkan banyak aturan terkait permasalahan perkembangan teknologi informasi, tidak hanya persoalan kejahatan teknologi informasi. EU juga telah mengatur masalah perdagangan elektronik yang terdiri atas: *The General EU Electronic Commerce Directive* – 4 Mei 2000, *Electronic Signature Directive* pada 30 November 1999 dan *Brussels Convention on Online Transactions,* yang berlaku 1 Maret 2002.

Directive 1999/93/EC merupakan kerangka hukum bagi tanda tangan elektronik dan pelayanan sertifikasi elektronik di Uni Eropa. Secara berlahan hampir 25 (dua puluh lima) negara EU telah mengadopsi prinsip-prinsip umum *Directive* 1999/93/EC. Tujuan dari *Directive* 1999/93/EC adalah untuk memudahkan penggunaan tanda tangan elektronik di negara-negara Uni Eropa dan sebagai pengakuan hukum penggunaan tanda tangan elektronik. *Directive* mendefinisikan tanda tangan elektronik sebagai data dalam bentuk elektronik yang terpasang atau terkait dengan data logis dan data elektronik lainnya dengan menggunakan metode otentikasi.

3. *General Usage for International Digitally Ensured Commerce* (GUIDEC) dari *International Chamber of Commerce* (ICC)

GUIDEC[43] adalah suatu panduan yang dibuat oleh *International Chamber of Commerce* bagi penggunaan suatu metode yang akan menjamin (*ensured*) keberadaan suatu dokumen/data elektronis dalam penggunaannya dalam dunia internasional. Panduan ini menggunakan terminologi *ensured* untuk membedakannya dengan terminologi *sign* dalam hal penandatanganan *(sign in / signature*) terhadap suatu dokumen. GUIDEC ini dimaksudkan untuk menunjang perkembangan dari *e-commerce* dengan memberikan kepastian bagi penerapan adanya tandatangan dalam suatu dokumen elektronis. Panduan ini akan menjelaskan berbagai terminologi/istilah yang ada didalam UNCITRAL *Model Law on E-commerce* seperti apakah sebenarnya maksud dari penandatangan suatu data *messages* secara elektronis (*electronically signed messages*). Maksud dari penandatanganan disini adalah bukan dilakukan secara fisik, tetapi membutuhkan suatu perangkat elektronik. Terminologi dari *electronically signed* yang dipakai dalam GUIDEC ini adalah penggunaan teknik enkripsi dengan menggunakan kunci publik yang lebih dikenal sebagai *digital signature*. Penggunaan *digital signature* ini akan memberikan kepastian akan keamanan, keutuhan dari data *messages* yang digunakan dalam *e-commerce*. Faktor keamanan dan keutuhan dari suatu data *messages* adalah suatu hal yang sangat menentukan dalam menunjang perkembangan *e-commerce*. *E-commerce* yang dilakukan melalui media internet yang merupakan suatu jaringan publik akan memberikan berbagai ketidakpastian bagi para penggunaanya. Dengan adanya suatu panduan mengenai bagaimana suatu data *messages* dapat dijamin keamanan dan keutuhan melalui cara *digital signature*.

B. KONSEP PENGATURAN *ELECTRONIC SIGNATURE* DI SINGAPURA

Singapura memiliki *Electronic Transactions Act* yang berlaku mulai tanggal 10 Juli 1998. Singapura merupakan negara pelopor *electronic signature* model *hybrid* di *The Third Wave* (Generasi Ketiga) serta baru saja pada tahun 2011 merubah peraturannya. ETA sebagai pengatur otoritas sertifikasi. Singapura mempunyai misi untuk menjadi poros / pusat kegiatan perdagangan elektronik internasional, dimana transaksi perdagangan yang elektronik dari daerah dan di seluruh bumi dapat diproses. *The Electronic Transactions Act* telah ditetapkan pada tanggal 10 Juli 1998 untuk menciptakan kerangka yang sah tentang undang-undang untuk transaksi perdagangan elektronik di Singapura yang memungkinkan bagi Menteri Informasi, Komunikasi dan Kesenian untuk membuat peraturan mengenai perijinan dan peraturan otoritas sertifikasi di Singapura.

Generasi Ketiga *E-Signature Law: Hybrid*

Pembuat undang-undang di Singapura dipengaruhi oleh UNCITRAL *Model Law on Electronic Commerce* 1996. Singapura mengadopsi model "*hybrid*" —acuan untuk *digital signature* dan PKI dalam pengertian yang lebih luas tentang *legal presumption of reliability* dan keamanan tetapi tidak pada pengecualian bentuk-bentuk lain dari *electronic signatures*. *Digital signature* lebih dihargai dalam perundang-undangan Singapura, tetapi tidak diberikan monopoli seperti dalam

[43] Lihat di http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2001/GUIDEC---General-Usage-for-International-Digitally-Ensured-Commerce-%28Version-II%29--01/10/2001/
Versi pertama GUIDEC dipublikasikan November 1997. Versi kedua GUIDEC dipublikasikan Oktober 2001.

generasi pertama. Teknologi yang terbuka ini berpandangan global dan memudahkan para pihak untuk melakukan transaksi elektronik dengan para pihak dari negara lain.

Meskipun memenuhi pengenalan legal terhadap berbagai jenis *e-signatures*, perundangan Singapura memberi anjuran keras kepada pengguna—dalam dua cara—bahwa mereka harus menggunakan *digital signature* karena lebih terpercaya dan lebih aman daripada jenis *e-signatures* lainnya :

(1) *digital signatures* dengan menggunakan PKI lebih dihargai dalam hukum pembuktian di pengadilan daripada jenis *E-signatures* lainnya, dan dokumen elektronik yang ditandatangani dengan *digital signatures* membawa legal presumption of reliability dan keamanan, dimana hal tersebut tidak diberikan pada jenis *E-signatures* lainnya; dan

(2) meskipun semua jenis *e-signatures* diperolehkan dipergunakan di Singapura, hukum *e-signature* memberikan aturan komprehensif untuk lisensi dan pengaturan *Certification Authorities* yang berperan penting untuk me-verifikasi *authenticity* dan *integrity* dari pesan elektronik yang melekat pada *electronic signatures*.

Semakin hari banyak Negara yang telah bergabung dengan Generasi Ketiga / *the Third Generation*. Posisi moderat yang diadopsi Singapore sekarang telah menjadi tren progresif dalam hukum *e-signature* internasional. Pendekatan *hybrid* yang dianut dalam *the European Union's E-Signatures Directive* 1999; Armenia[44]; Azerbaijan; Barbados; Bermuda, Bulgaria; China; Kolombia; Kroasia; Dubai; Finland; Hong Kong; Hungaria; Iran; Jepang; Lithuania; Pakistan; Peru; Slovenia; Korea Selatan; Taiwan; Tunisia; Vanuatu; dan Uganda sedang dalam rancangan undang-undang. Banyak negara lain yang sekarang menggunakan pendekatan *hybrid* atau sedang menimbang untuk mengadopsinya, salah satunya adalah Birma.

Pasal 2 SETA[45]

"digital signature" means 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 signer"s public key; and

(b) whether the initial electronic record has been altered since the transformation was made.

"electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record.

Dalam website IDA[46] dikatakan bahwa

"digital signature is an electronic form of a real world hand-written signature. Instead of applying to paper documents, digital signatures are applied to

---

[44] Stephen E. Blythe, *Armenia's Electronic Document And Electronic Signature Law : Promotion Of Growth In E-commerce Via Greater Cyber-Security* Lihat di http://law.aua.am/pdf/esignaturelaw.pdf

[45] Lihat di http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan025623.pdf diunduh pada tanggal 29 Juli 2012 pukul 21.00 WIB

[46] Lihat di http://www.ida.gov.sg/Policies%20and%20Regulation/20060920100740.aspx diunduh tanggal 29 Juli 2012 pukul 20.00 WIB

electronic documents. Like hand-written signatures, digital signatures can be used to prove the authenticity of electronic documents. Someone who reads a document that is digitally signed by you can be assured that the document came from you. In addition, he is also assured of the integrity of the document, i.e., the document is complete and has not been modified in any way".

Pasal 3 SETA[47] mengatur tujuan pembuatan SETA yaitu :

a. Memudahkan komunikasi elektronik atas pertolongan arsip elektronik yang dapat dipercaya.

b. Memudahkan perdagangan elektronik, yaitu menghapuskan penghalang perdagangan elektronik yang tidak sah atas penulisan dan persyaratan tandatangan, dan untuk mempromosikan pengembangan dari undang-undang dan infrastruktur bisnis diperlukan untuk menerapkan menjamin / mengamankan perdagangan elektronik.

c. Memudahkan penyimpanan secara elektronik tentang dokumen pemerintah dan perusahaan.

---

[47] *3. This Act shall be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes:*

(a) to facilitate electronic communications by means of reliable electronic records;

(b) to facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

(c) to facilitate electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of reliable electronic records;

(d) to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;

(e) to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records; and

(f) to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

Lihat di *http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan025623.pdf* diunduh tanggal 29 Juli 2012 pukul 21.05 WIB

d. Meminimalkan timbulnya arsip elektronik yang sama (*double*), perubahan yang tidak disengaja dan disengaja tentang arsip, dan penipuan dalam perdagangan elektronik dan lain-lain.

e. Membantu menuju keseragaman aturan, peraturan dan mengenai pengesahan dan integritas dari arsip elektronik.

f. Mempromosikan kepercayaan, integritas dan keandalan dari arsip elektronik dan perdagangan elektronik, dan untuk membantu perkembangan dan pengembangan dari perdagangan elektronik melalui penggunaan tandatangan yang elektronik untuk menjamin keaslian dan integritas surat menyurat yang menggunakan media elektronik.

Pasal 4 SETA mengatur aplikasi dalam praktek bahwa

(1) Parts II[48] and IV[49] shall not apply to any rule of law requiring writing or signatures in any of the following matters :

(a) the creation or execution of a will;

(b) negotiable instruments;

(c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts;

(d) any contract for the sale or other disposition of immovable property, or any interest in such property;

(e) the conveyance of immovable property or the transfer of any interest in immovable property;

(f) documents of title.

(2) The Minister may by order modify the provisions of subsection (1) by adding, deleting or amending any class of transactions or matters.

Dalam Bagian II *electronic records* dan *signatures* secara umum :

Pasal 6 tentang *legal recognition of electronic records*

For the avoidance of doubt, it is declared that information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

Pasal 7 tentang *requirement for writing*

Where a rule of law requires information to be written, in writing, to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule of law if the information contained therein is accessible so as to be usable for subsequent reference.

Pasal 8 SETA mengatur

(1) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in

---

[48] *ELECTRONIC RECORDS AND SIGNATURES GENERALLY*

[49] *ELECTRONIC CONTRACTS*

order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.

SETA juga menjelaskan bahwa pengadilan tidak boleh tertutup hanya pada metode tradisional untuk membuktikan *electronic signatures*. Pengadilan boleh mempercayai pembuktian termasuk bukti eksekusi dari simbol atau bukti prosedur keamanan untuk tujuan meverifikasi bahwa dokumen elektronik tersebut ditanda tangani oleh yang bersangkutan.

Pasal 17 tentang *secure electronic signature*

If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made —

(a) unique to the person using it;

(b) capable of identifying such person;

(c) created in a manner or using a means under the sole control of the person using it; and

(d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated, such signature shall be treated as a secure electronic signature.

Pasal 20 mengatur mengenai masalah *secure digital signatures*[50]. Penggunaan *secure digital signatures* ini untuk meyakinkan keamanan dari sertifikat atau keaslian data yang menyertainya. Dengan menggunakan *secure digital signatures* ini maka keamanan akan dapat lebih terjamin mengingat sifat unik dari *secure digital signatures* ini sehingga tidak memungkinkan suatu peniruan oleh pihak lain.

Pasal 22 tentang *unreliable digital signatures*

Unless otherwise provided by law or contract, a person relying on a digitally signed electronic record assumes the risk that the digital signature is invalid as a signature or authentication of the signed electronic record, if reliance on the digital signature is not reasonable under the circumstances having regard to the following factors :

(a) facts which the person relying on the digitally signed electronic record knows or has notice of, including all facts listed in the certificate or incorporated in it by reference;

---

[50] *When any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the record, if —*

(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate; and

(b) the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity because —

(i) the certificate was issued by a licensed certification authority operating in compliance with the regulations made under section 42 ;

(ii) the certificate was issued by a certification authority outside Singapore recognised for this purpose by the Controller pursuant to regulations made under section 43;

(iii) the certificate was issued by a department or ministry of the Government, an organ of State or a statutory corporation approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or

(iv) the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

(b) the value or importance of the digitally signed electronic record, if known;

(c) the course of dealing between the person relying on the digitally signed electronic record and the subscriber and any available indicia of reliability or unreliability apart from the digital signature; and

(d) any usage of trade, particularly trade conducted by trustworthy systems or other electronic means.

Bagian VII mengatur tentang kewajiban umum berkaitan dengan *digital signatures* :

Pasal 23 tentang *reliance on certificates foreseeable*

It is foreseeable that persons relying on a digital signature will also rely on a valid certificate containing the public key by which the digital signature can be verified.

Pasal 24 tentang *prerequisites to publication of certificate*

No person may publish a certificate or otherwise make it available to a person known by that person to be in a position to rely on the certificate or on a digital signature that is verifiable with reference to a public key listed in the certificate, if that person knows that —

(a) the certification authority listed in the certificate has not issued it;

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been suspended or revoked, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

C. PERBANDINGAN KONSEP PENGATURAN *ELECTRONIC SIGNATURE* DI *UNCITRAL'S UNIFORM RULES ON ELECTRONIC SIGNATURES* DAN SINGAPORE'S *ELECTRONIC TRANSACTIONS ACT*

Berikut ini merupakan analisa perbandingan hukum regulasi - regulasi internasional yang mengatur mengenai *electronic signature* (tanda tangan elektronik) dari UNCITRAL dengan *Electronic Transactions Act* dari Singapura sebagai berikut:

1. Definisi tanda tangan elektronik

Pasal 2 ayat (a) UNCITRAL *Model Law on Electronic Signature* mendefinisikan sebagai berikut :

"Electronic signature" means data in electronic form in, affixed to or logically associaied with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message."

Pasal 2 SETA[51]

"digital signature" means 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 signer"s public key; and

---

[51] Lihat di http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan025623.pdf diunduh pada tanggal 29 Juli 2012 pukul 21.00 WIB

(b) whether the initial electronic record has been altered since the transformation was made.

"electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record.

UNCITRAL *Model Law on Electronic Signature* mendefinisikan bahwa tanda tangan elektronik merupakan suatu data elektronik yang terasosiasi dengan suatu pesan data yang dapat digunakan unluk mengidentifikasi penandatangan dalam kaitannya pesan data dan mengindikasikan persetujuan penanda tangan terhadap suatu informasi yang terkandung dalam pesan data tersebut.

Pada hakikatnya ketiga regulasi tersebut mendefinisikan hal yang sama mengenai tanda tangan elektronik. Dimana dari ketiga regulasi tersebut dapat disimpulkan bahwa yang dimaksud dengan tanda tangan elektronik adalah suatu data elektronik baik berupa suara, simbol maupun proses yang terasosiasi dengan sebuah pesan data yang mengindikasikan persetujuan penandatangan.

Dengan demikian jelas bahwa pada dasarnya definisi tanda tangan elektronik yang terdapat dalam *Singapore's Electronic Transactions Act* merupakan implementasi dari aturan yang terdapat dalam UNCITRAL *Model Law* tersebut.

Tanda tangan elektronik dan tanda tangan digital pada hakikatnya adalah tidak sama. Tanda tangan elektronik berarti tidak hanya berupa tanda tangan yang menggunakan teknik kriptografi, melainkan juga termasuk tanda tangan konvensional yang di-*digitalized* menggunakan *scanner*. Pada dasarnya *digital signature* merupakan bagian dari tanda tangan elektronik.

2. Persyaratan tanda tangan elektronik

Persyaratan tanda tangan elektronik yang diatur dalam Pasal 7 ayat (1) UNCITRAL *Model Law on Electronic Commerce* sebagai berikut:

"Where the law requires a signature of a person, that requirement is met in a relation to a data message if:

a. A method is used to identify that person and to indicate that person's approval of the information contained in the data message

b. That method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement"

Pasal 6 ayat (3) UNCITRAL *Model Law on Electronic Signature* mengatur syarat tanda tangan elektronik sebagai berikut :

"An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if :

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any

alteration made to that information after the time of signing is detectable".

Pasal 8 SETA mengatur *electronic signatures*

(1) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.

3. Pengakuan atas tanda tangan elektronik

Pasal 3 UNCITRAL *Model Law on Electronic Signature* :

" Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6, paragraph 1, or otherwise meets the requirements of applicable law."

Pasal 6 (3) UNCITRAL *Model Law on Electronic Signature* mengatur syarat tanda tangan elektronik sebagai berikut :

a. The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

b. The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

c. Any alteration to the electronic signature, made after the time of signing, is detectable; and

d. Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

Pasal 8 SETA mengatur

(1) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.

SETA juga menjelaskan bahwa pengadilan tidak boleh tertutup hanya pada metode tradisional untuk membuktikan *electronic signatures*. Pengadilan boleh mempercayai pembuktian termasuk bukti eksekusi dari simbol atau bukti prosedur keamanan untuk tujuan meverifikasi bahwa dokumen elektronik tersebut ditanda tangani oleh yang bersangkutan.

Pasal 17 tentang *secure electronic signature*

If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made —

(a) unique to the person using it;
(b) capable of identifying such person;
(c) created in a manner or using a means under the sole control of the person using it; and
(d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated, such signature shall be treated as a secure electronic signature.

Pasal 20 mengatur mengenai masalah *secure digital signatures*[52]. Penggunaan *secure digital signatures* ini untuk meyakinkan keamanan dari sertifikat atau keaslian data yang menyertainya. Dengan menggunakan *secure digital signatures* ini maka keamanan akan dapat lebih terjamin mengingat sifat unik dari *secure digital signatures* ini sehingga tidak memungkinkan suatu peniruan oleh pihak lain.

Pasal 22 tentang *unreliable digital signatures*

Unless otherwise provided by law or contract, a person relying on a digitally signed electronic record assumes the risk that the digital signature is invalid as a signature or authentication of the signed electronic record, if reliance on the digital signature is not reasonable under the circumstances having regard to the following factors :

(a) facts which the person relying on the digitally signed electronic record knows or has notice of, including all facts listed in the certificate or incorporated in it by reference;
(b) the value or importance of the digitally signed electronic record, if known;
(c) the course of dealing between the person relying on the digitally signed electronic record and the subscriber and any available indicia of reliability or unreliability apart from the digital signature; and
(d) any usage of trade, particularly trade conducted by trustworthy systems or other electronic means.

Dengan demikian dapat disimpulkan bahwa tanda tangan elektronik yang digunakan sebagai alat pengaman dalam hal pertukaran data/informasi elektronik memiliki kedudukan serta akibat hukum. Hal ini berarti bahwa penggunaan *digital signature* dalam transaksi elektronik dilindungi hukum karena itulah dapat diakui dalam persidangan.

---

[52] *When any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the record, if —*

(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate; and
(b) the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity because —
  (i) the certificate was issued by a licensed certification authority operating in compliance with the regulations made under section 42 ;
  (ii) the certificate was issued by a certification authority outside Singapore recognised for this purpose by the Controller pursuant to regulations made under section 43;
  (iii) the certificate was issued by a department or ministry of the Government, an organ of State or a statutory corporation approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or
  (iv) the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

Berdasarkan persamaan-persamaan dasar dalam pengaturan tanda tangan digital sebagaimana diuraikan diatas dapat dikemukakan bahwa tanda tangan digital memiliki kedudukan hukum dalam regulasi internasional. Negara sebagai lingkup yang lebih kecil sewajarnya memiliki pula aturan hukum yang dapat menjamin kenyamanan. kepastian, serta keamanan dalam bertransaksi elektronik melalui *digital signature* sebagai media pengamannya. Di Singapura, transaksi elektronik diatur dalam *Electronic Transactions Act*.

PENUTUP

A. KESIMPULAN

1. Pengaturan *electronic signature* di Singapura

Electronic signature di Singapura diatur dalam *Electronic Transactions Act* yang berlaku mulai tanggal 10 Juli 1998. Singapura merupakan negara pelopor *electronic signature* model *hybrid* di *The Third Wave* (Generasi Ketiga) serta baru saja pada tahun 2011 merubah peraturannya. Pembuat undang-undang di Singapura dipengaruhi oleh UNCITRAL *Model Law on Electronic Commerce* 1996. Singapura mengadopsi model "*hybrid*" —acuan untuk *digital signature* dan PKI dalam pengertian yang lebih luas tentang *legal presumption of reliability* dan keamanan tetapi tidak pada pengecualian bentuk-bentuk lain dari *electronic signatures*. Meskipun memenuhi pengenalan legal terhadap berbagai jenis *e-signatures*, perundangan Singapura memberi anjuran keras kepada pengguna—dalam dua cara—bahwa mereka harus menggunakan *digital signature* karena lebih terpercaya dan lebih aman daripada jenis *e-signatures* lainnya :

(1) *digital signatures* dengan menggunakan PKI lebih dihargai dalam hukum pembuktian di pengadilan daripada jenis *E-signatures* lainnya, dan dokumen elektronik yang ditandatangani dengan *digital signatures* membawa legal presumption of reliability dan keamanan, dimana hal tersebut tidak diberikan pada jenis *E-signatures* lainnya; dan

(2) meskipun semua jenis *e-signatures* diperolehkan dipergunakan di Singapura, hukum *e-signature* memberikan aturan komprehensif untuk lisensi dan pengaturan *Certification Authorities* yang berperan penting untuk me-verifikasi *authenticity* dan *integrity* dari pesan elektronik yang melekat pada *electronic signatures*.

Isi SETA mencakup hal-hal berikut :

a. Kontrak Elektronik : didasarkan pada hukum dagang *online* yang dilakukan secara wajar dan cepat serta untuk memastikan bahwa kontrak elektronik memiliki kepastian hukum.

b. Kewajiban Penyedia Jasa Jaringan : mengatur mengenai potensi / kesempatan yang dimiliki oleh *network service provider* untuk melakukan hal-hal yang tidak diinginkan, seperti mengambil, membawa, menghancurkan material atau informasi pihak ketiga yang menggunakan jasa jaringan tersebut. Pemerintah Singapura merasa perlu untuk mewaspadai hal tersebut.

c. Tandatangan dan Arsip elektronik : Hukum memerlukan arsip/bukti arsip elektronik untuk menangani kasus-kasus elektronik, karena itu tandatangan dan arsip elektronik tersebut harus sah menurut hukum.

SETA juga menjelaskan bahwa pengadilan tidak boleh tertutup hanya pada metode tradisional untuk membuktikan *electronic signatures*. Pengadilan boleh mempercayai pembuktian termasuk bukti eksekusi dari simbol atau bukti prosedur keamanan untuk tujuan meverifikasi bahwa dokumen elektronik tersebut ditanda tangani oleh yang bersangkutan.

2. Perbandingan pengaturan *electronic signature* di Singapura dengan *UNCITRAL's Uniform Rules on Electronic Signatures*

a. Definisi tanda tangan elektronik

Pada hakikatnya kedua regulasi tersebut mendefinisikan hal yang sama mengenai tanda tangan elektronik. Dimana dari ketiga regulasi tersebut dapat disimpulkan bahwa yang dimaksud dengan tanda tangan elektronik adalah suatu data elektronik baik berupa suara, simbol maupun proses yang terasosiasi dengan sebuah pesan data yang mengindikasikan persetujuan penandatangan. Dengan demikian jelas bahwa pada dasarnya definisi tanda tangan elektronik yang terdapat dalam *Singapore's Electronic Transactions Act* merupakan implementasi dari aturan yang terdapat dalam UNCITRAL *Model Law* tersebut.

Tanda tangan elektronik dan tanda tangan digital pada hakikatnya adalah tidak sama. Tanda tangan elektronik berarti tidak hanya berupa tanda tangan yang menggunakan teknik kriptografi, melainkan juga termasuk tanda tangan konvensional yang di-*digitalized* menggunakan *scanner*. Pada dasarnya *digital signature* merupakan bagian dari tanda tangan elektronik.

b. Persyaratan tanda tangan elektronik yang diatur dalam Pasal 7 ayat (1) UNCITRAL *Model Law on Electronic Commerce* sebagai berikut:

"Where the law requires a signature of a person, that requirement is met in a relation to a data message if:

a. A method is used to identify that person and to indicate that person's approval of the information contained in the data message

b. That method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement"

Pasal 6 ayat (3) UNCITRAL *Model Law on Electronic Signature* mengatur syarat tanda tangan elektronik sebagai berikut :

"An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if :

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any

alteration made to that information after the time of signing is detectable".

Pasal 8 SETA mengatur *electronic signatures*

(1) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.

c. Pengakuan atas tanda tangan elektronik

Pasal 3 UNCITRAL *Model Law on Electronic Signature* :

" Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6, paragraph 1, or otherwise meets the requirements of applicable law."

Pasal 6 (3) UNCITRAL *Model Law on Electronic Signature* mengatur syarat tanda tangan elektronik sebagai berikut :

a. The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

b. The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

c. Any alteration to the electronic signature, made after the time of signing, is detectable; and

d. Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

Pasal 8 SETA mengatur

(1) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.

SETA juga menjelaskan bahwa pengadilan tidak boleh tertutup hanya pada metode tradisional untuk membuktikan *electronic signatures*. Pengadilan boleh mempercayai pembuktian termasuk bukti eksekusi dari simbol atau bukti prosedur keamanan untuk tujuan meverifikasi bahwa dokumen elektronik tersebut ditanda tangani oleh yang bersangkutan.

Pasal 17 tentang *secure electronic signature*

If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made —

(a) unique to the person using it;
(b) capable of identifying such person;
(c) created in a manner or using a means under the sole control of the person using it; and
(d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated, such signature shall be treated as a secure electronic signature.

Pasal 20 mengatur mengenai masalah *secure digital signatures*[53]. Penggunaan *secure digital signatures* ini untuk meyakinkan keamanan dari sertifikat atau keaslian data yang menyertainya. Dengan menggunakan *secure digital signatures* ini maka keamanan akan dapat lebih terjamin mengingat sifat unik dari *secure digital signatures* ini sehingga tidak memungkinkan suatu peniruan oleh pihak lain.

Pasal 22 tentang *unreliable digital signatures*

Unless otherwise provided by law or contract, a person relying on a digitally signed electronic record assumes the risk that the digital signature is invalid as a signature or authentication of the signed electronic record, if reliance on the digital signature is not reasonable under the circumstances having regard to the following factors :

(a) facts which the person relying on the digitally signed electronic record knows or has notice of, including all facts listed in the certificate or incorporated in it by reference;
(b) the value or importance of the digitally signed electronic record, if known;
(c) the course of dealing between the person relying on the digitally signed electronic record and the subscriber and any available indicia of reliability or unreliability apart from the digital signature; and
(d) any usage of trade, particularly trade conducted by trustworthy systems or other electronic means.

Dengan demikian dapat disimpulkan bahwa tanda tangan elektronik yang digunakan sebagai alat pengaman dalam hal pertukaran data/informasi elektronik memiliki kedudukan serta akibat hukum. Hal ini berarti bahwa penggunaan *digital signature* dalam transaksi elektronik dilindungi hukum karena itulah dapat diakui dalam persidangan.

---

[53] *When any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the record, if —*
(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate; and
(b) the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity because —
(i) the certificate was issued by a licensed certification authority operating in compliance with the regulations made under section 42 ;
(ii) the certificate was issued by a certification authority outside Singapore recognised for this purpose by the Controller pursuant to regulations made under section 43;
(iii) the certificate was issued by a department or ministry of the Government, an organ of State or a statutory corporation approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or
(iv) the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

B. SARAN

Diperlukan suatu perumusan dan pemberlakuan ketentuan pelaksana yang mengatur keberadaan para pelaku usaha yang bersedia menjadi pengemban amanat kepercayaan lokal untuk penjaminan resiko dalam penyelenggaraan transaksi perdagangan secara elektronik serta penyuluhan hukum kepada masyarakat untuk mensosialisasikan istilah *electronic signature* serta *digital signature* dan penggunaan *electronic signature* dalam menghadapi kemajuan di bidang perdagangan dan teknologi.

DAFTAR PUSTAKA

Buku

Attig, et. al. *A Field Manual on Selected QualitativeResearch Methods* (Thailand: Institute for Population and Social Research, Mahidol University, 1991

Bambang Waluyo. *Penelitian Hukum Dalam Praktek*. Jakarta : Sinar Grafika, 1996.

C.F.G. Sunaryati Hartono. *Penelitian Hukum Di Indonesia Pada Akhir Abad Ke-20.* Bandung : Alumni, 1994.

Enid Campbell, et. al., *Legal Research, Materials and Methods.* Sydney: The Law Book Company Limited, 1988.

Soerjono Soekanto dan Sri Mamudji. *Penelitian Hukum Normatif : Suatu Tinjauan Singkat.* Cet-Kelima, Jakarta : Raja Grafindo Persada, 2001.

Soerjono Soekanto. *Pengantar Penelitian Hukum*. Cet. 3.,Jakarta : UI Press, 1986.

Situs Internet

http://hukumperdatainternasionalbisnis.wordpress.com/

http://id.wikipedia.org/wiki/Singapura

http://law.aua.am/pdf/esignaturelaw.pdf

http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan025623.pdf

http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan025623.pdf

http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan025623.pdf

http://www.bogor.net/idkf/onno/raw-data/digital-review-of-asia-pacific/manuscript/3.08-regulatory-environment/dprin.go.id/ruu-tte.pdf

http://www.gpo.gov/fdsys/pkg/BILLS-106s761enr/pdf/BILLS-106s761enr.pdf

http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2001/GUIDEC---General-Usage-for-International-Digitally-Ensured-Commerce-%28Version-II%29--01/10/2001/

http://www.ida.gov.sg/Policies%20and%20Regulation/20060920100740.aspx

http://www.ilpf.org/groups/analysis_IEDSII.htm

http://www.informatika.org/~rinaldi/Kriptografi/Makalah/Makalah12.pdf

http://www.singaporelaw.sg/content/LegalSystIndon.html

http://www.stephenmason.eu/e-signatures/

http://www.stephenmason.eu/e-signatures/biodynamic-signature/

http://www.stephenmason.eu/e-signatures/click-wrap/

http://www.stephenmason.eu/e-signatures/digital-signature/

http://www.stephenmason.eu/e-signatures/name-in-e-mail-address/

http://www.stephenmason.eu/e-signatures/pin/

http://www.stephenmason.eu/e-signatures/scanned-manuscript-signature/

http://www.stephenmason.eu/e-signatures/typing-a-name-in-an-electronic-document/

http://www.umt.edu.pk/icobm/proceedings/pdf/Paper29.pdf

http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

www.geocities.com/amwibowo/resource/hukum/hukum_set.pdf

Peraturan

The UNCTTRAL Model law on Electronic Commerce
The UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001
The General EU Electronic Commerce Directive – 4 Mei 2000
Electronic Signature Directive pada 30 November 1999
Brussels Convention on Online Transactions
General Usage for International Digitally Ensured Commerce (GUIDEC) , *International Chamber of Commerce* (ICC)
Singapore's *Electronic Transactions Act 2011*
Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, disahkan,diundangkan dan mulai berlaku tanggal 21 April 2008, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.