TINJAUAN YURIDIS TENTANG PERJANJIAN ELEKTRONIK YANG MENGGUNAKAN PENYELENGGARA SERTIFIKASI ELEKTRONIK (*CERTIFICATE AUTHORITY* ATAU CA) ASING

TESIS

SUCI LESTARI

6505001009

UNIVERSITAS INDONESIA

FAKULTAS HUKUM

PROGRAM PASCASARJANA

SALEMBA, JAKARTA

JULI 2008

TINJAUAN YURIDIS TENTANG PERJANJIAN ELEKTRONIK YANG MENGGUNAKAN PENYELENGGARA SERTIFIKASI ELEKTRONIK (*CERTIFICATE AUTHORITY* ATAU CA) ASING

TESIS

Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Hukum

SUCI LESTARI

6505001009

UNIVERSITAS INDONESIA

FAKULTAS HUKUM

PROGRAM STUDI ILMU HUKUM

BIDANG HUKUM EKONOMI

SALEMBA, JAKARTA

JULI 2008

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri,

dan semua sumber , baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama	**:**	**Suci Lestari**
NPM	**:**	**6505001009**
Tanda Tangan	**:**	
Tanggal	**:**	**25 Juli 2008**

HALAMAN PENGESAHAN

Tesis ini diajukan oleh	:	
Nama	:	Suci Lestari
NPM	:	6505001009
Program Studi	:	Ilmu Hukum
Judul Tesis	:	Tinjauan Yuridis Tentang Perjanjian Elektronik Yang Menggunakan Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA) Asing

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

DEWAN PENGUJI

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

Penguji : Ratih Lestarini, S.H., M.H. (.....)

Penguji : Dr. Inosentius Samsul, S.H., M.H. (.....)

Ditetapkan di : Jakarta

Tanggal : 25 Juli 2008

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

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

Nama	:	Suci Lestari
NPM	:	6505001009
Program Studi	:	Ilmu Hukum
Departemen	:	
Fakultas	:	Hukum
Jenis Karya	:	Tesis

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

Tinjauan Yuridis Tentang Perjanjian Elektronik Yang Menggunakan Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA) Asing

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-eksklusif ini, Universitas Indonesia berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 25 Juli 2008

Yang menyatakan

(Suci Lestari)

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan anugerah-Nya, saya dapat menyelesaikan penulisan tesis yang berjudul "Tinjauan Yuridis Tentang Perjanjian Elektronik Yang Menggunakan Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA) Asing" ini. Penulisan tesis ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Magister Hukum pada Program Pascasarjana Fakultas Hukum Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan tesis ini, sangatlah sulit bagi saya untuk menyelesaikan tesis ini. Oleh karena itu, saya mengucapkan terima kasih kepada :

1. Bapak Edmon Makarim, S.H., S.Kom, LL.M. selaku dosen pembimbing yang telah bersedia memberikan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan tesis ini;

2. Bapak Josua Sitompul, S.H. selaku asisten Bapak Edmon di Departemen Komunikasi dan Informasi yang telah membagi bahan-bahan untuk tesis saya;

3. Bapak Endar Pulungan, SH MH selaku Dekan Fakultas Hukum Universitas Trisakti yang telah memberikan kesempatan kepada saya untuk melanjutkan studi ke jenjang strata dua;

4. Bapak H. Hasni, SH MH selaku mantan Wakil Dekan I FH USAKTI, Bapak Dhany Rahmawan, SH MH selaku Wakil Dekan I FH USAKTI, Ibu Hj. Muriani, SH MH selaku mantan Wakil Dekan II FH USAKTI, Ibu Irene Mariane, SH CN MH selaku Wakil Dekan II Fakultas Hukum Universitas Trisakti, Ibu Lusi dan Ibu Ratya Sesara yang selalu membantu saya dalam pencairan dana studi;

5. Staf Perpustakaan Fakultas Hukum Universitas Trisakti, Ibu Ade Alfay Nur, Ibu Darwini, Bapak Agung dan Bapak Budi S yang telah membantu saya dengan meminjamkan buku-buku yang penulis butuhkan selama studi dan penulisan tesis;

6. Staf Administrasi Program Pascasarjana Fakultas Hukum Universitas Indonesia, Pak Watijan, Pak Ari, Pak Huda, dan lain-lain yang sudah membantu penulis selama masa studi penulis;

7. Teman-teman, Ibu Andari Yurikosari, SH MH, Bapak Arif Wicaksana, SH MH, Irene Anatola, SE dan lainnya yang telah membantu saya selama studi dalam dukungan moral dan sebagainya;

8. Papa, Alianda Halim, yang selalu mendukung, mendoakan dan memberi nasehat kepada penulis, adik-adik, Indah Ningsih Lestari Halim dan Johanes Halim, yang selalu mendukung penulis dalam doa;

9. Hie Victor, suami penulis, terima kasih atas saran, dukungan, doa serta nasehat selama penulis menjalankan studi dan masa penulisan tesis, yang selama ini telah sangat sabar memberikan perhatian, kasih sayang dan dorongan yang tiada hentinya kepada penulis;

10. Kepada pihak-pihak lain yang tidak dapat saya sebutkan satu persatu.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga tesis ini dapat membawa manfaat bagi pengembangan ilmu.

Ciledug, Juli 2008

Penulis

ABSTRAK

Nama : Suci Lestari

Program Studi : Ilmu Hukum

Judul : Tinjauan Yuridis Tentang Perjanjian Elektronik Yang Menggunakan Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA) Asing

Tesis ini membahas bagaimana status perjanjian elektronik menurut Hukum Indonesia, bagaimana transaksi yang melibatkan Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau C.A.) dan bagaimana pengaturan lisensi Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA) asing di Indonesia dibandingkan dengan negara-negara lain misalnya Uni Eropa (UE) atau *European Union* (EU), Inggris, Amerika, Singapura dan Malaysia ? Penelitian ini adalah penelitian kualitatif dengan metode penelitian kepustakaan dengan data sekunder sebagai sumber datanya. Penulisan tesis ini merupakan upaya untuk menggambarkan penggunaan penyelenggara sertifikasi elektronik asing dikaitkan dengan status perjanjian tersebut dalam transaksi elektronik, serta menunjukkan bahwa penggunaan penyelenggara sertifikasi elektronik yang tidak mempunyai izin operasi/lisensi membawa akibat hukum dalam perjanjian elektronik yang bersangkutan. Ketiadaan izin operansi/lisensi dari C.A. mengakibatkan status tandatangan elektronik dalam perjanjian elektronik yang bersangkutan tidak mempunyai kekuatan hukum yang sama seperti status tandatangan elektronik dalam perjanjian elektronik yang menggunakan C.A. yang mempunyai izin operasi/lisensi dan terakreditasi. Peraturan lisensi mengenai C.A. di Indonesia yang dibandingkan dengan peraturan di negara lainnya memberikan beberapa masukan untuk perubahan peraturan pelaksana mengenai C.A. di Indonesia.

Kata kunci :

perjanjian elektronik, penyelenggara sertifikasi elektronik

ABSTRACT

Name : Suci Lestari

Study Program : Ilmu Hukum

Title : Legal Review On Electronic Contract Using Foreign Certificate Authority

This thesis discussing how the status of electronic contract according Indonesia's Law, what transaction that using certificate authority or C.A. and how the licensing regulation of foreign certificate authority or C.A. in Indonesia compare with at other countries such as European Union (EU), Great Britain, United States of America, Washington States, Singapore and Malaysia ? This research is a qualitative research with method of literature research with secondary data as its data source. This writing thesis is an effort to describe that the status of certificate authority giving impact to the status of the electronic contract, and showing that using unlicensed certificate authority bring legal impact at the electronic contract itself. Unlicense certificate authority making status of electronic sign in that electronic contract does not have same electronic sign's status like that using license and accredited certificate authority. The license regulation on certificate authority in Indonesia that compare with regulation at other countries giving some ideas for the changing of C.A. regulation in Indonesia.

Key words :

electronic contract, certificate / certification authority

DAFTAR ISI

DAFTAR GAMBAR

BAB 1

PENDAHULUAN

1.1. LATAR BELAKANG PERMASALAHAN

Perekonomian dunia mengalami perubahan sejak dasawarsa tujuh puluh hingga tahun 2000-an yang bersifat mendasar atau struktural dan mempunyai kecenderungan jangka panjang atau konjungtural untuk terus mengalami perubahan. Perkembangannya sangat menarik untuk terus diikuti, jika meminjam istilah yang popular belakangan ini adalah "globalisasi[1]".

Gejala globalisasi terjadi dalam seluruh kegiatan pembangunan, baik dari segi finansial, produksi, investasi, dan perdagangan yang kemudian mempengaruhi tata hubungan ekonomi antar bangsa. Proses globalisasi itu telah meningkatkan kadar hubungan saling ketergantungan antar negara, bahkan menimbulkan proses menyatunya ekonomi dunia, sehingga "batas-batas antar negara dalam berbagai praktek dunia usaha/bisnis seakan-akan dianggap tidak berlaku lagi"[2].

Perkembangan teknologi informasi dan telekomunikasi yang semakin konvergen (terpadu) dewasa ini, telah mengakibatkan semakin beragamnya pula aneka jasa-jasa (*features*) fasilitas telekomunikasi yang ada, serta semakin canggihnya produk-produk teknologi informasi yang mampu mengintegrasikan semua media informasi. Di tengah globalisasi komunikasi yang semakin terpadu

---

[1] Ade Maman Suherman, *Aspek Hukum Dalam Ekonomi Global*, Cet.Pertama (Jakarta: Ghalia Indonesia, 2002), hal. 31.mengutip pendapat Dicken (1992) yaitu *globalization is more usually described in the business literature as a shifts in traditional patterns of international production, investment and trade* (globalisasi lazimnya lebih digambarkan dalam literature bisnis sebagai suatu penggantian pola tradisional dalam produksi internasional, investasi dan perdagangan).

[2] Hendra Halwani, *Ekonomi Internasional & Globalisasi Ekonomi*, (Jakarta : Ghalia Indonesia, 2005), hal. 224.

(*global communication network*) ditambah lagi dengan semakin populernya penggunaan internet seolah-olah telah membuat dunia semakin menciut (*shrinking the world*). Hal ini membawa dampak semakin memudarnya batas-batas negara berikut kedaulatan dan tatananan masyarakatnya. Ironisnya, dinamika masyarakat Indonesia yang masih baru tumbuh dan berkembang sebagai masyarakat industri dan masyarakat informasi, seolah masih tampak prematur untuk mengiringi perkembangan teknologi tersebut[3].

Komputer sebagai alat bantu manusia dengan didukung perkembangan teknologi informasi telah membantu akses ke dalam jaringan publik (*public network*) agar dapat melakukan pemindahan data dan informasi. Dengan kemampuan komputer dan akses yang semakin berkembang maka transaksi perdagangan pun dilakukan di dalam jaringan komunikasi tersebut. Jaringan publik mempunyai keunggulan dibandingkan dengan jaringan privat dengan adanya efisiensi biaya dan waktu. Hal ini membuat perdagangan dengan transaksi elektronik (*electronic commerce*) menjadi pilihan bagi para pelaku bisnis untuk melancarkan transaksi perdagangannya karena sifat jaringan publik yang mudah untuk diakses oleh setiap orang ataupun perusahaan.

Pesatnya perkembangan teknologi pada umumnya, teknologi informasi khususnya, telah mendorong terjadinya kompleksitas hubungan atau transaksi dagang internasional, oleh dan antar pelaku *(subjek hukum)* dalam perdagangan internasional, yang bersifat lintas dan menembus batas-batas negara (*transnasional)*, serta perbedaan sistem hukum, sistem politik dan lain-lain dari dan antar pelaku dalam perdagangan internasional tersebut, misalnya dengan kelangsungan suatu transaksi-transaksi lintas negara yang berlangsung cepat[4].

---

[3] Group Riset UI, "Kerangka Hukum Digital Signature dalam *Electronic Commerce*", (Hasil penelitian oleh group riset *digital* dan *security* dan *electronic* yang pernah dipresentasikan di hadapan Masyarakat Telekomunikasi Indonesia di Pusat Ilmu Komputer Universitas Indonesia, Depok, Jawa Barat, Juni 1999.,tersedia di http://www.geocities.com/amwibowo/resource/.htm

[4] Huala Adolf, *Hukum Perdagangan Internasional*, Cet.2., (Jakarta : PT.Rajagrafindo Persada, 2006), hal.1-3.

Pada pokoknya, yang menjadi perubahan besar dengan hadirnya sistem *e-commerce*[5] adalah terjadinya perubahan cara/mekanisme transaksi perdagangan yang semula dengan alternatif metode transaksi yang berdasarkan kertas (*paper-based methods*) menjadi transaksi yang berdasarkan komunikasi elektronis (*communication and storage of information*)[6].

Para pelaku perdagangan melalui transaksi elektronik (*electronic commerce*) yang memanfaatkan fasilitas internet, di mana dalam pelaksanaannya menimbulkan banyak permasalahan, salah satunya permasalahan di bidang hukum yaitu transaksi perdagangan yang dilakukan melalui media internet yang tidak mengenal batas-batas antar negara apakah mendapat perlindungan hukum ? Sebagai antisipasi dari pelaksanaan perdagangan melalui transaksi elektronik (*electronic commerce*) yang *borderless*, negara-negara di dunia membuat perlindungan hukum dalam bentuk pembuatan regulasi, persiapan infrastruktur dan aparat pelaksananya.

Globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa. Perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah mempengaruhi lahirnya bentuk-bentuk perbuatan hukum baru. Hal tersebut diikuti oleh Indonesia dengan membuat regulasi yang

---

[5] *E–Commerce (Konsep Perdagangan Dunia Maya dan Aspek Hukumnya)*, Bandung : Materi *powerpoint* Hukum Bisnis Genap 2007-2008 Universitas Kristen Maranatha, tersedia di *hukbis.files.wordpress.com/2008/04/e-commerce-ver-2003.ppt* Terdapat 6 (enam) komponen dalam *Electronic Commerce Transaction* (Kontrak Dagang Elektronik) yaitu ada kontrak dagang, kontrak itu dilaksanakan dengan media elektronik, kehadiran fisik dari para pihak tidak diperlukan, kontrak itu terjadi dalam jaringan publik, menggunakan sistem terbuka, yaitu dengan internet atau www. dan kontrak itu terlepas dari batas yurisdiksi nasional.

[6] Edmon Makarim, *Kerangka Hukum Untuk Kebijaksanaan Dan Pengaturan Sektor Jasa Telekomunikasi Untuk Transaksi Perdagangan Secara Elektronik (Legal Framework: Policy and Regulation of Electronic Commerce)*, 1999 tersedia di www.bogor.net/idkf/idkf/aplikasi/Copy%20of%20hukum-dan-warfare/mastel-regulasi-2B.doc

mengatur tentang Informasi dan Transaksi Elektronik dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik[7]. Dengan diundangkannya UU ini maka diharapkan transaksi perdagangan dengan model transaksi elektronik (*electronic transaction*) mendapatkan perlindungan hukum secara pasti.

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

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 yangdikirim dan diterima tidak berubah *(Integrity);* dan pihak yang terkait tidak dapat menyangkal telah melakukan transaksi *(Non- Repudiation).*

---

[7] Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, disahkan,diundangkan dan mulai berlaku tanggal 21 April 2008, Tambahan Lembaran Negara Republik Indonesia Nomor 4843. Budi Rahardjo dalam *Panduan Cyberlaw Untuk Orang Biasa (Idiot's Guide to Indonesian Cyberlaw),* http://budi.insan.co.id/articles/panduan-cyberlaw.pdf, hal.3., berpendapat bahwa RUU ITE ini merupakan ***Umbrela Provision*** yang dibuat berdasarkan pendekatan top down dan global yang diharapkan ada landasan yang kuat untuk membuat UU atau PP yang lebih spesifik lainnya(misalnya khusus untuk Digital Signature, khusus tentang e-Banking, khusus tentang e-Government,dan UU/PP yang khusus lainnya.

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 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, mensyaratkan keterlibatan pihak ketiga terpercaya *(Trusted Third Party)* yang independen.

Pihak ketiga terpercaya akan membantu menjamin otentikasi subyek hukum yang membuat transaksi melalui internet atau identitas dari para pihak pelaku transaksi elektronik melalui infrastruktur kunci publik dan menyediakan mekanisme untuk melakukan transaksi elektronik secara aman. Selanjutnya pihak ketiga terpercaya akan memberikan layanan tersebut melalui suatu institusi yang lazim dikenal sebagai *Certification Authority* (CA)[8]. CA menerbitkan Sertifikat Digital[9]

---

[8] Lampiran Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2006 tentang Pedoman Penyelenggaraan *Certification Authority* di Indonesia, hal. 5. memberikan pengertian dari terminologi *Certification Authority* (CA) adalah sebuah badan hukum yang berfungsi sebagai pihak ketiga terpercaya yang menerbitkan SD dan menyediakan keamanan yang dapat dipercaya oleh para pengguna dalam menjalankan pertukaran informasi secara elektronis sehingga memenuhi 4 (empat) aspek keamanan yaitu : 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 di jamin otentisitasnya *(Authentication);* informasi yang dikirim dan diterima tidak berubah *(integrity);* dan pihak yang terkait tidak dapat menyangkal telah melakukan transaksi *(Non Repudiation).*

Catatan : Karena pihak ketiga tidak memiliki kepentingan terhadap transaksi yang dilakukan oleh pihak pertama dan kedua, maka ia dapat bersikap independen dan tidak memihak.

Bandingkan dengan definisi yang terdapat di Pasal 1 butir (10) UU ITE No. 11 Tahun 2008 yaitu yang dimaksud dengan Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.

[9] *Ibid.* Lampiran Permeninfo ini juga memberikan pengertian dari terminologi Sertifikat Digital (SD) adalah sertifikat yang terikat dengan kunci publik terhadap suatu subjek (pengguna). Sertifikat tersebut

(Digital Certificate) yang digunakan para pihak untuk menyatakan identitasnya dalam melakukan transaksi elektronik[10].

Dalam hal ini keberadaan *Certification Authority* (CA) penting untuk membangun kepercayaan melalui pelaksanaan otentifikasi terhadap identitas para pihak yang terlibat dalam transaksi secara online dan menyajikan bukti tentang pengiriman berbagai pesan melalui internet dan melakukan verifikasi terhadap integritas informasi yang dipertukarkan[11]. Keabsahan kontrak juga sangat krusial/penting karena keabsahan kontrak menentukan apakah suatu perjanjian itu berlaku atau tidak, mengikat atau tidak, untuk para pihak yang membuat perjanjian tersebut.

Dalam pembahasan tesis ini penulis membatasi pada penggunaan Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA) Asing yang disyaratkan dalam Pasal 13 Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) harus terdaftar di Indonesia dikaitkan dengan status perjanjian dalam transaksi bisnis yang dilakukan melalui media elektronik.

Sementara untuk acuan yuridis dari transaksi elektronik dan CA tersebut maka penulis mengacu pada Kitab Undang-Undang Hukum Perdata (KUHPer), UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), *UNCITRAL Model Law on E-Commerce*[12] dan konvensi internasional lainnya, *European Union*

---

dikeluarkan oleh CA dengan menggunakan kunci pribadi dari CA. Berisi data, kunci publik dan konfirmasi identitas pemegang kunci publik (pengguna) dan ditandatangani oleh CA.

Bandingkan dengan definisi yang terdapat di Pasal 1 butir (9) UU ITE No. 11 Tahun 2008 yaitu yang dimaksud dengan Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan
identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan olehPenyelenggara Sertifikasi Elektronik.

[10] *Ibid.*, hal. 1-2.

[11] Kata Pengantar Direktur Jenderal Aplikasi Telematika tentang Pedoman Penyelenggaraan Certification Authority di Jakarta, 2 Februari 2007 tersedia di *http://www.depkominfo.go.id/portal/?act=detail&mod=program&view=1&id=7*

[12] The United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce diadopsi dalam Sidang Umum PBB pada tanggal 16 Desember 1996, G.A. Res.

Directive, peraturan di Inggris, Amerika, Negara Bagian Washington, Singapura dan Malaysia serta peraturan lainnya yang berkaitan.

Atas dasar hal tersebutlah, penulis tertarik untuk menelitinya lebih lanjut dan memilih judul tesis: **"Tinjauan Yuridis Tentang Perjanjian Elektronik Yang Menggunakan Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA) Asing".**

1.2. PERUMUSAN MASALAH

Berangkat dari latar belakang permasalahan tersebut diatas, maka dapat dirumuskan pokok permasalahan dalam penulisan ini, yaitu membahas mengenai:

a. Bagaimana status perjanjian elektronik menurut Hukum Indonesia ?
b. Bagaimana transaksi yang melibatkan Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA)?
c. Bagaimana pengaturan tentang izin operasi / lisensi Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA) asing di Indonesia dibandingkan dengan di Negara lainnya misalnya Uni Eropa (UE) atau *European Union* (EU), Inggris, Amerika, Negara Bagian Washington, Singapura dan Malaysia ?

1.3. TUJUAN DAN KEGUNAAN PENELITIAN

Adapun tujuan dari penulisan yang dilakukan adalah sebagai berikut :

51/162, U.N.Doc. A/RES/51/162 (Dec. 16, 1996), dengan tambahan Pasal 5 bis yang diadopsi tahun 1998 tersedia di *http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf*

UNCITRAL sebagai salah satu badan Perserikatan Bangsa-Bangsa yang bergerak dalam perdagangan internasional merumuskan suatu model hukum dalam *e-commerce.*

Yang dimaksud dengan Model law dalam leaflet UNCITRAL adalah "a set of model legislative provisions that States can adopt by enacting it into national law". Tersedia di *http://www.uncitral.org/pdf/english/uncitral-leaflet-e.pdf*

A. Tujuan Umum :

Penulisan ini secara umum bertujuan untuk mendapatkan gambaran secara teoritis dan praktis mengenai aspek hukum perjanjian elektronik yang menggunakan penyelenggara sertifikasi elektronik (*Certificate Authority* atau CA) asing.

B. Tujuan Khusus :

1) Untuk mengetahui bagaimana status perjanjian elektronik menurut Hukum Indonesia.
2) Untuk mengetahui bagaimana transaksi yang melibatkan Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA).
3) Untuk mengetahui bagaimana pengaturan tentang izin operasi / lisensi Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA) asing di Indonesia dibandingkan dengan di Negara lainnya misalnya Uni Eropa (UE) atau *European Union* (EU), Inggris, Amerika, Negara Bagian Washington, Singapura dan Malaysia.

Adapun kegunaan penelitian ini dibagi menjadi 2 (dua) tujuan sebagai berikut:

A. Kegunaan Teoritis

1) dapat memberikan kontribusi bagi pengembangan literatur hukum pada umumnya dan kajian hukum perdagangan pada khususnya;
2) dapat mendorong peneliti lain untuk lebih lanjut mengembangkan kajian atau memperkuat konsep-konsep yang dihasilkan oleh penelitian ini, sehingga diharapkan akan membawa masukan berarti bagi ilmu pengetahuan Teknologi Telekomunikasi, Media dan Informatika ("TELEMATIKA") dan memperkaya pengetahuan hukum perdagangan Indonesia.

B. Kegunaan Praktis

1) dapat menambah wawasan bagi para Sarjana Hukum baik praktisi, akademisi, maupun *in-house lawyer* dan masyarakat umum dalam pemahaman dan menghadapi masalah-masalah yang berkaitan dengan hukum perjanjian elektronik;

2) dapat menjadi salah satu bahan masukan dan pertimbangan bagi pemerintah dalam pembuatan peraturan pelaksana dari Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang yang berkaitan lainnya.

1.4. METODE PENELITIAN

Dalam penelitian ini akan digunakan metode penelitian sebagai berikut :

1. Tipe Penelitian

Tipe penelitian yang digunakan dalam penelitian ini adalah tipe penelitian hukum normatif. Alasan digunakannya tipe penelitian hukum normatif adalah bahwa penelitian ini berbasis pada analisis terhadap norma hukum, baik hukum dalam arti *law as it is written in the books* (dalam peraturan perundang-undangan), maupun hukum dalam arti *law as it is decided by the judge through judicial process* (putusan-putusan pengadilan)[13]. 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 literatur-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[14].

---

[13] Ronald Dworkin, *Legal Research*, (Daedalus : Spring, 1973), hal.250.

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

2. Sifat Penelitian

Jika ditinjau dari sifatnya, maka penelitian ini bersifat *deskriptif-analitis*. Hal tersebut didasarkan pada alasan bahwa tujuan dilaksanakannya penelitian ini adalah untuk memberikan data yang selengkap-lengkapnya dan seteliti mungkin, khususnya data mengenai aspek hukum perjanjian perdagangan dalm transaksi elektronik. Selain memberikan deskripsi, maka dalam penelitian ini juga menganalisis tentang masalah-masalah apa saja yang timbul dari perjanjian elektronik yang menggunakan penyelenggara sertifikasi elektronik asing.

3. Data Penelitian

Dalam penelitian ini, maka peneliti menggunakan data sekunder yang pada umumnya tersedia dalam bentuk literatur-literatur tertulis dan bersifat publik yang telah siap digunakan. Karakteristik lain dari data sekunder tersebut bahwa selain bentuk maupun isinya telah dibentuk dan diisi oleh peneliti-peneliti terdahulu, maka data sekunder juga dapat diakses tanpa terikat atau dibatasi oleh waktu dan tempat[15]. Adapun data sekunder dalam penelitian hukum ini terdiri dari[16] :

a. Bahan hukum primer, yaitu berupa bahan-bahan hukum yang mengikat dan terdiri dari peraturan dasar (UUD 1945 dan Ketetapan MPR), peraturan perundang-undangan khususnya yang terkait dan mengatur mengenai bidang pertanahan, bahan hukum yang tidak dikodifikasikan seperti hukum adat dan lain-lain.
b. Bahan hukum sekunder, yaitu berupa bahan-bahan hukum yang memberikan penjelasan mengenai bahan hukum primer, seperti rancangan undang-undang,

[15] Soerjono Soekanto dan Sri Mamudji, *Op.Cit.*, hal.24. Lebih lanjut dijelaskan bahwa pada dasarnya, penggunaan data sekunder dalam suatu penelitian mempunyai kegunaan yang berupa adanya penghematan biaya dan tenaga, adanya posibilitas untuk memperkokoh dan memperluas dasar-dasar penarikan suatu generalisasi dan dapat menimbulkan gagasan-gagasan yang lebih baru. Selain itu, penggunaan data sekunder juga memiliki kelemahan yang berupa kesulitan untuk mengetahui secara tepat lokasi terhimpunnya data sekunder tersebut, perlu adanya kegiatan sistematisasi kembali sesuai dengan sistematika dan kerangka penelitian yang sedang dilakukan oleh peneliti dan adanya kesulitan untuk mengetahui secara pasti bagaimana proses pengumpulan dan pengolahan data sekunder yang dihadapi.

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

hasil-hasil penelitian yang tersaji dalam bentuk laporan, hasil karya dari kalangan hukum yang berupa buku, majalah serta artikel atau makalah ilmiah dan lain-lain.

c. Bahan hukum tersier, yaitu bahan-bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder, seperti kamus, ensiklopedia, bibliografi, indeks kumulatif dan lain-lain.

4. Alat atau Cara Pengumpulan Data.

Untuk memperoleh data sekunder maka peneliti menggunakan alat pengumpulan berupa studi dokumen (*documentary study*). Penggunaan studi dokumen tersebut dilakukan dengan cara menganalisis substansi atau isi (*content analysis*) dari data atau bahan-bahan tertulis yang berhasil didapat dan dikumpulkan oleh penulis[17].

5. Analisis Data Penelitian.

Pemilihan terhadap analisis yang tepat digunakan dalam suatu penelitian hendaknya selalu didasarkan pada tipe, tujuan dan jenis data yang terkumpul. Apabila data yang diperoleh tersebut lebih bersifat pengukuran maka analisis yang tepat digunakan adalah kuantitatif. Sebaliknya, apabila data yang diperoleh tersebut sulit untuk dilakukan pengukuran dengan angka-angka maka analisis yang digunakan adalah bersifat kualitatif. Selain itu, penggunaan analisis kualitatif juga dapat dilakukan terhadap data yang diperoleh dari proses wawancara yang dilakukan dengan berdasarkan pada pedoman wawancara. Dengan demikian, pada penelitian ini, maka peneliti menggunakan analisis kualitatif terhadap data yang telah diperoleh.

1.5. KERANGKA TEORI DAN KERANGKA KONSEPTUAL

Berbicara mengenai transaksi jual beli secara elektronik, tidak terlepas dari konsep perjanjian secara mendasar sebagaimana termuat dalam Pasal 1313 KUH Perdata yang menegaskan bahwa perjanjian adalah suatu perbuatan dengan mana

---

[17] *Ibid.*, hal.21.

satu orang atau lebih mengikatkan dirinya terhadap satu orang lain atau lebih. Ketentuan yang mengatur tentang perjanjian terdapat dalam Buku III KUH Perdata, yang memiliki sifat terbuka artinya ketentuan-ketentuannya dapat dikesampingkan, sehingga hanya berfungsi mengatur saja. Sifat terbuka dari KUH Perdata ini tercermin dalam Pasal 1338 ayat (1) KUH Perdata yang mengandung asas Kebebasan Berkontrak, maksudnya setiap orang bebas untuk menentukan bentuk, macam dan isi perjanjian asalkan tidak bertentangan dengan peraturan perundang-undangan yang berlaku, kesusilaan dan ketertiban umum, serta selalu memperhatikan syarat sahnya perjanjian sebagaimana termuat dalam Pasal 1320 KUH Perdata yang mengatakan bahwa, syarat sahnya sebuah perjanjian adalah sebagai berikut :

1. Kesepakatan para pihak dalam perjanjian
2. Kecakapan para pihak dalam perjanjian
3. Suatu hal tertentu
4. Suatu sebab yang halal

Kesepakatan berarti adanya persesuaian kehendak dari para pihak yang membuat perjanjian, sehingga dalam melakukan suatu perjanjian tidak boleh ada paksaan, kekhilafan dan penipuan *(dwang, dwaling, bedrog)*.

Kecakapan hukum sebagai salah satu syarat sahnya perjanjian maksudnya bahwa para pihak yang melakukan perjanjian harus telah dewasa yaitu telah berusia 18 tahun atau telah menikah, sehat mentalnya serta diperkenankan oleh undang-undang. Apabila orang yang belum dewasa hendak melakukan sebuah perjanjian, maka dapat diwakili oleh orang tua atau walinya sedangkan orang yang cacat mental dapat diwakili oleh pengampu atau kuratornya[18].

Suatu hal tertentu berhubungan dengan objek perjanjian, maksudnya bahwa objek perjanjian itu harus jelas, dapat ditentukan dan diperhitungkan jenis dan jumlahnya, diperkenankan oleh undang-undang serta mungkin untuk dilakukan para pihak.

---

[18] Riduan Syahrani, *Seluk-Beluk Dan Asas-Asas Hukum Perdata*, (Bandung:Alumni, 1992), hal.217.

Suatu sebab yang halal, berarti perjanjian termaksud harus dilakukan berdasarkan itikad baik. Berdasarkan Pasal 1335 KUH Perdata, suatu perjanjian tanpa sebab tidak mempunyai kekuatan. Sebab dalam hal ini adalah tujuan dibuatnya sebuah perjanjian[19].

Kesepakatan para pihak dan kecakapan para pihak merupakan syarat sahnya perjanjian yang bersifat subjektif. Apabila tidak tepenuhi, maka perjanjian dapat dibatalkan artinya selama dan sepanjang para pihak tidak membatalkan perjanjian, maka perjanjian masih tetap berlaku. Sedangkan suatu hal tertentu dan suatu sebab yang halal merupakan syarat sahnya perjanjian yang bersifat objektif. Apabila tidak terpenuhi, maka perjanjian batal demi hukum artinya sejak semula dianggap tidak pernah ada perjanjian.

Pada dasarnya suatu perjanjian harus memuat beberapa unsur perjanjian yaitu[20]:

1. unsur *essentialia*, sebagai unsur pokok yang wajib ada dalam perjanjian, seperti identitas para pihak yang harus dicantumkan dalam suatu perjanjian, termasuk perjanjian yang dilakukan jual beli secara elektronik.
2. unsur *naturalia*, merupakan unsur yang dianggap ada dalam perjanjian walaupun tidak dituangkan secara tegas dalam perjanjian, seperti itikad baik dari masing-masing pihak dalam perjanjian.
3. unsur *accidentalia*, yaitu unsur tambahan yang diberikan oleh para pihak dalam perjanjian, seperti klausula tambahan yang berbunyi "barang yang sudah dibeli tidak dapat dikembalikan".

Dalam suatu perjanjian harus diperhatikan pula beberapa macam azas yang dapat diterapkan antara lain :

---

[19] *Ibid*, hal.218.

[20] Lihat R. Setiawan, *Pokok-Pokok Hukum Perikatan*, Cet.Ketiga, (Bandung : Binacipta, 1986), hal. 50.

1. Azas Konsensualisme, yaitu azas kesepakatan, dimana suatu perjanjian dianggap ada seketika setelah ada kata sepakat.
2. Azas Kepercayaan, yang harus ditanamkan diantara para pihak yang membuat perjanjian.
3. Azas kekuatan mengikat, maksudnya bahwa para pihak yang membuat perjanjian terikat pada seluruh isi perjanjian dan kepatutan yang berlaku.
4. Azas Persamaan Hukum, yaitu bahwa setiap orang dalam hal ini para pihak mempunyai kedudukan yang sama dalam hukum.
5. Azas Keseimbangan, maksudnya bahwa dalam melaksanakan perjanjian harus ada keseimbangan hak dan kewajiban dari masing-masing pihak sesuai dengan apa yang diperjanjikan.
6. Azas Moral adalah sikap moral yang baik harus menjadi motivasi para pihak yang membuat dan melaksanakan perjanjian.
7. Azas Kepastian Hukum yaitu perjanjian yang dibuat oleh para pihak berlaku sebagai undang-undang bagi para pembuatnya.
8. Azas Kepatutan maksudnya bahwa isi perjanjian tidak hanya harus sesuai dengan peraturan perundang-undangan yang berlaku tetapi juga harus sesuai dengan kepatutan, sebagaimana ketentuan Pasal 1339 KUH Perdata yang menyatakan bahwa suatu perjanjian tidak hanya mengikat untuk hal-hal yang dengan tegas dinyatakan didalamnya, tetapi juga untuk segala sesuatu yang menurut sifat perjanjian diharuskan oleh kepatutan, kebiasaan atau undang-undang.
9. Azas Kebiasaan, maksudnya bahwa perjanjian harus mengikuti kebiasaan yang lazim dilakukan, sesuai dengan isi Pasal 1347 KUH Perdata yang berbunyi hal-hal yang menurut kebiasaan selamanya diperjanjikan dianggap secara diam-diam dimasukkan ke dalam perjanjian, meskipun tidak dengan tegas dinyatakan. Hal ini merupakan perwujudan dari unsur naturalia dalam perjanjian.

Semua ketentuan perjanjian tersebut diatas dapat diterapkan pula pada perjanjian yang dilakukan melalui media internet, seperti perjanjian jual beli secara elektronik, sebagai akibat adanya perkembangan ilmu pengetahuan dan teknologi.

Secara umum pemasalahan-permasalahan yang timbul pada transaksi elektronik mencakup : keabsahannya, saat terjadinya kontrak, syarat tertulis, syarat tanda tangan, masalah pembuktian. Sama seperti sahnya perjanjian / kontrak pada umumnya, keabsahan suatu transaksi elektronis sebenarnya tidak perlu diragukan lagi sepanjang terpenuhinya syarat-syarat kontrak. Dalam sistem hukum Indonesia, sepanjang terdapat kesepakatan diantara para pihak; cakap mereka yang membuatnya; atas suatu hal tertentu; dan berdasarkan suatu sebab yang halal, maka transaksi tersebut seharusnya sah, meskipun melalui proses elektronis. Untuk mendukung pandangan tersebut, dalam lingkup internasional terdapat beberapa ketentuan yang dapat menjadi acuan, antara lain[21]:

> *The United Nations Conference on International Trade Law (UNCITRAL) Model Law on E-Commerce of 1996*, yang merumuskan bahwa akibat, keabsahan atau dapat ditegakkannya suatu informasi tidak dapat disangkal semata-mata karena formatnya sebagai pesan data (data message);
>
> *The European Union (EU) Directive on E-Commerce of 2000*: menegaskan bahwa negara anggotanya wajib menjamin bahwa sistem hukum mereka memungkinkan kontrak dibuat dengan sarana elektronis;
>
> *Singapore's E-Transaction Act of 1998*: merumuskan bahwa untuk menghindari keraguan, dinyatakan bahwa informasi tidak dapat disangkal akibat hukumnya, keabsahannya maupun kemampuan untuk ditegakkannya semata-mata dengan alasan bahwa informasi tersebut dalam bentuk rekaman elektronis.

Electronic Commerce (Perniagaan Elektronik), sebagai bagian dari *Electronic Business* (bisnis yang dilakukan dengan menggunakan *electronic transmission*, oleh para ahli dan pelaku bisnis dicoba dirumuskan definisinya dari terminologi *E-*

---

[21] I.B.R Supancana, *Kekuatan Akta Elektronis Sebagai Alat Bukti Pada Transaksi E-Commerce Dalam Sistem Hukum Indonesia, http://www.indoregulation.com/.*

Commerce (Perniagaan Elektronik). Secara umum *e-commerce* dapat didefinisikan sebagai segala bentuk transaksi perdagangan/perniagaan barang atau jasa (*trade of goods and service*) dengan menggunakan media elektronik. Jelas, selain dari yang telah disebutkan di atas, bahwa kegiatan perniagaan tersebut merupakan bagian dari kegiatan bisnis. Kesimpulan: "e-*commerce is a part of e-business*"[22].

Media elektronik yang dibicarakan di dalam tesis ini hanya difokuskan dalam hal penggunaan media internet, mengingat penggunaan media internet yang saat ini paling populer digunakan oleh banyak orang, selain merupakan hal yang bisa dikategorikan sebagai hal yang sedang '*booming*'. Perlu digarisbawahi, dengan adanya perkembangan teknologi di masa mendatang, terbuka kemungkinan adanya penggunaan media jaringan lain selain internet dalam *e-commerce*. Jadi pemikiran kita jangan hanya terpaku pada penggunaan media internet belaka.

Penggunaan internet dipilih oleh kebanyakan orang sekarang ini karena kemudahan-kemudahan yang dimiliki oleh jaringan internet :

1. Internet sebagai jaringan publik yang sangat besar (*huge/widespread network*), layaknya yang dimiliki suatu jaringan publik elektronik, yaitu murah, cepat dan kemudahan akses.
2. Menggunakan *electronic* data sebagai media penyampaian pesan/data sehingga dapat dilakukan pengiriman dan penerimaan informasi secara mudah dan ringkas, baik dalam bentuk data elektronik analog maupun digital.

Dari apa yang telah diuraikan di atas, dengan kata lain; di dalam *e-commerce*, para pihak yang melakukan kegiatan perdagangan/perniagaan hanya berhubungan

---

[22] Arya Indra W, *Mengenal E-commerce*, tugas makalah komputer, Fakultas Kedokteran Universitas Jember, 2007, tersedia di *http://www.elearning.unej.ac.id/courses/KD225/work/466f560f31aceMengenal_E-com.doc*

melalui suatu jaringan publik (*public network*) yang dalam perkembangan terakhir menggunakan media internet[23].

Pertukaran informasi melalui media elektronik (internet) yang terkait dengan transaksi bisnis atau perdagangan secara elektronik memerlukan pengamanan melalui Infrastruktur Kunci Publik (IKP) agar informasi yang diperlukan memenuhi persyaratan *privacy / confidentiality, authentication, integrity* dan *non repudiation.* Fakta menunjukkan bahwa perubahan pesan- pesan elektronik dapat dilakukan dengan mudah dan tidak terdeteksi, sehingga meningkatkan resiko terjadinya manipulasi terhadap pesan elektronik yang dikirim. Dengan meningkatnya penggunaan internet, akan meningkatkan pula resiko kecurangan, penipuan, serta akses ilegal.

Dalam rangka menimbulkan kepercayaan dan kepastian hukum bagi pengguna terhadap sistem komunikasi dengan internet, diperlukan suatu keterlibatan pihak ketiga terpercaya (*trusted third party*) yang independen untuk mengelola resiko termasuk penggunaan IKP. *Trusted third party* yang akan membantu menjamin identitas para pihak pelaku transaksi elektronik melalui IKP dan menyediakan mekanisme untuk melakukan transaksi elektronik secara aman. *Trusted third party* tersebut adalah sebagai *Certification Authority* (CA) yang menerbitkan Sertifikat Digital yang digunakan para pihak untuk menyatakan identitasnya dalam melakukan transaksi elektronik.

1.6. SISTEMATIKA PENULISAN

Maksud dan tujuan dari sistematika penulisan ini adalah untuk memudahkan dan memberikan gambaran secara keseluruhan materi penulisan dengan pembahasannya.

---

[23] *http://www.geocities.com/amwibowo/resource/hukum_ttd/hukum_ttd.html* diakses pada tanggal 3 Januari 2008 pukul 18:00.

Tesis ini akan disusun dan disajikan dalam 5 (lima) bab, dimana dalam setiap bab dibagi menjadi beberapa sub bab lagi. Pembagian tersebut dilakukan secara sistematis sesuai dengan tahap-tahap uraian sehingga bab-bab tersebut tidak berdiri sendiri melainkan berhubungan satu sama lainnya yang merupakan satu kesatuan yang menyeluruh. Selengkapnya kerangka permasalahan yang akan dibahas setiap bab secara sistematis, dengan urutan pembahasan sebagai berikut :

Bab Pertama merupakan Bab Pendahuluan yang terdiri dari 6 (enam) sub bab, yaitu tentang Latar Belakang Permasalahan, Rumusan Masalah, Tujuan dan Kegunaan Penelitian, Metode Penelitian, Kerangka Teori dan Kerangka Konseptual, dan diakhiri dengan Sistematika Penulisan.

Bab Kedua merupakan bagian yang akan membahas Status Perjanjian Dalam Transaksi Elektronik, yang terdiri dari 2 (dua) sub bab. Sub bab pertama mengenai Tinjauan Umum Tentang Perjanjian dalam Sistem *Common Law* dan Sistem *Civil Law* yang terdiri dari kontrak menurut *common law* atau *Anglo Saxon*, kontrak menurut *civil law* atau Eropa Kontinental dan tinjauan umum tentang perjanjian di Indonesia yang terdiri dari pengertian perjanjian, sifat terbuka perjanjian, unsur-unsur dalam perjanjian, asas-asas dalam hukum perjanjian. Diakhiri dengan sub bab kedua yang membahas mengenai Tinjauan Umum Tentang Perjanjian dalam Transaksi Elektronik yang terdiri dari pengertian *electronic commerce*, pengaturan kontrak *e-commerce* dalam konvensi internasional, dan tinjauan umum tentang transaksi elektronik yang terdiri dari pengertian transaksi elektronik, persyaratan hukum dalam komunikasi *online*.

Bab Ketiga merupakan bagian yang akan menjelaskan Transaksi Elektronik yang melibatkan Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA), yang terdiri dari 2 (dua) sub bab. Sub bab pertama terdiri dari pembahasan Konsep Infrastruktur Kunci Publik (*Public Infrastructure Key*) yang terdiri dari konsep dasar kriptografi, kriptografi kunci simetrik, kriptografi kunci publik / kunci asimetrik, fungsi *hash* satu arah, tanda tangan digital, tanda tangan elektronik, sertifikat digital, transaksi elektronik dengan kriptografi. Diakhiri dengan sub bab

kedua mengenai *Certificate Authority* (C.A.) Sebagai *Trusted Third Party* Dalam Transaksi Elektronik.

Bab Keempat merupakan bab yang akan menjelaskan Pengaturan Izin Operasi / Lisensi Penyelenggara Sertifikasi Elektronik (*Certificate Authority* atau CA) Asing yang terdiri dari 3 (tiga) sub bab. Sub bab pertama mengenai Tinjauan Umum Tentang Izin Operasi/Lisensi C.A. yang terdiri dari Pentingnya izin operasi/lisensi C.A., Pentingnya pendaftaran C.A. dan Dampak ijin operasi/lisensi dan akreditasi terhadap status tandatangan elektronik. Dan dilanjutkan dengan sub bab kedua mengenai Status Perjanjian Elektronik Yang Menggunakan Penyelenggara Sertifikasi Elektronik (*Certificate Authority* Atau C.A.) Asing ditinjau dari permasalahan Keabsahan (*Validity*), Pelaksanaan *(Enforceability)* dan Pengakuan *(Admisibility)* perjanjian elektroniknya. Dan diakhiri dengan sub bab ketiga yang membahas tentang Perbandingan Pengaturan Izin Operasi / Lisensi Penyelenggara Sertifikasi Elektronik (*Certificate Authority* Atau CA) Asing Di Indonesia dengan negara lainnya seperti Uni Eropa, Inggris, Amerika Serikat, Negara Bagian Washington, Singapura dan Malaysia dimana pengaturan tesebut di Uni Eropa terdapat dalam *EU Directive* 1999/93/EC pada 13 Desember 1999 Tentang Tanda Tangan Elektronik, di Negara Inggris dalam *Electronic Communications Act* 2000 dan *the Electronic Signatures Regulations* 2002 (*the Regulations)*, di Amerika Serikat dalam *Uniform Electronic Transactions Act* (UETA) 1999, Negara Bagian Washington dalam *Chapter* 19.34. *Electronic Authentication Act* 1997, Singapura dalam *Electronic Transactions Act,* Malaysia dalam *Digital Signature Act (DSA)* serta pengaturan C.A. secara nasional di Indonesia dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2006 tentang Pedoman Penyelenggaraan *Certification Authority* di Indonesia dan Peraturan Menteri Komunikasi dan Informatika No. 30 Tahun 2006 tentang Badan Pengawas *Certification Authority*.

Bab kelima merupakan bab penutup dari tulisan ini yang terdiri dari 2 (dua) sub bab yaitu Kesimpulan dan Saran.

BAB 2
STATUS PERJANJIAN DALAM TRANSAKSI ELEKTRONIK

2.1. TINJAUAN UMUM TENTANG PERJANJIAN DALAM SISTEM *COMMON LAW* DAN *CIVIL LAW*

Secara garis besar di dunia ini meskipun dikenal ada lima sistem hukum, yaitu; *common law, civil law, socialist law, islamic law* dan sistem hukum adat, tetapi sesungguhnya yang dominan dipakai di dunia internasional hanyalah dua, yaitu sistem hukum *civil law* dan *common law.*

Dalam pembentukan kontrak, terdapat perbedaan antara *common law* dan *civil law.* Akibat perbedaan ini sangat mempengaruhi dalam penyusunan ketentuan kontrak internasional.

Sehubungan dengan perbedaan dalam sistem hukum tersebut, maka kemudian dalam rangka merancang suatu kontrak atau pembuatan suatu konsep perjanjian pun dengan sendirinya mengacu pada sistem hukum yang dianut[24]. Namun zaman terus bergerak, dan tiba saatnya era globalisasi yang juga mau tidak mau mempengaruhi sistem hukum yang diterapkan, apabila terjadi perjumpaan antara sistem hukum yang berlainan.

Transaksi elektronik menyebabkan para pihak dalam kontrak mungkin berasal dari berbagai sistem hukum yang berbeda. Dalam kerangka ini, perlu dianalisis kecocokan karakter hukum perjanjian di Indonesia dengan karakter hukum kontrak lainnya, dalam hal ini karakter hukum kontrak di dalam *common law system.*

---

[24] Ida Bagus Wyasa Putra dkk., *Hukum Bisnis Pariwisata* (Bandung:PT. Refika Aditama, 2001) Dalam tradisi *common law*, sahnya suatu kontrak ditentukan oleh keseriusan proses negosiasi, sedangkan pada *civil law* ditentukan oleh pernyataan kehendak untuk terikat (*expression of will*) para pihak.

2.1.1. Kontrak menurut *Common Law* atau *Anglo Saxon*[25]

Common law system berkembang di sebagian besar Inggris sebagai hasil dari kegiatan pengadilan di daerah-daerah di Inggris, sehingga hukum yang terbentuk bukan merupakan undang-undang hasil parlemen tetapi berdasarkan kasus *(law is not based on act of parliament but on case law)* yang ditangani hakim dalam memutuskan suatu kasus hukum (*judge made law*[26]). Melalui putusan-putusan hakim inilah diwujudkan kepastian hukum, sehingga prinsip-prinsip dan kaidah hukum terbentuk menjadi kaidah yang mengikat umum.

Selain putusan-putusan hakim, *common law system* juga mengakui kebiasaan, peraturan tertulis, undang-undang dan peraturan administrasi negara. Hanya semua itu tidak tersusun dalam bentuk yang sistematik dan hirarkis seperti halnya sistem hukum Eropa Kontinental (*civil law system*) yang menekankan pentingnya kodifikasi.

Menurut sistem *common law*, pembentukan perjanjian mengharuskan dipenuhinya 4(empat) syarat, yaitu :

a. *An agreement*/kesepakatan para pihak untuk mengikatkan diri, mencakup:

---

[25] Sistem Anglo-Saxon adalah suatu sistem hukum yang didasarkan pada yurisprudensi, yaitu keputusan-keputusan hakim terdahulu yang kemudian menjadi dasar putusan hakim-hakim selanjutnya. Sistem hukum ini diterapkan di Irlandia, Inggris, Australia, Selandia Baru, Afrika Selatan, Kanada (kecuali Provinsi Quebec) dan Amerika Serikat (walaupun negara bagian Louisiana mempergunakan sistem hukum ini bersamaan dengan sistim hukum Eropa Kontinental Napoleon). Selain negara-negara tersebut, beberapa negara lain juga menerapkan sistem hukum Anglo-Saxon campuran, misalnya Pakistan, India dan Nigeria yang menerapkan sebagian besar sistem hukum Anglo-Saxon, namun juga memberlakukan hukum adat dan hukum agama.

Sistem hukum Anglo-Saxon, sebenarnya penerapannya lebih mudah terutama pada masyarakat pada negara-negara berkembang karena sesuai dengan perkembangan zaman. Pendapat para ahli dan prakitisi hukum lebih menonjol digunakan oleh hakim, dalam memutus perkara.

Dapat dilihat di *http://id.wikipedia.org/wiki/Hukum*

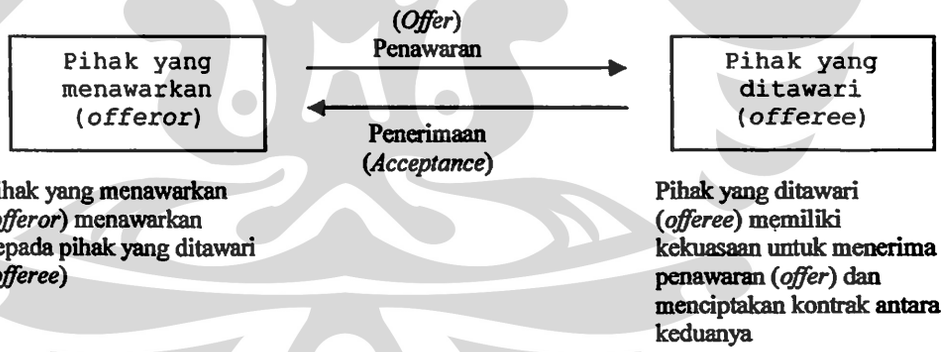
[26] Menurut Steven Vago, *Law is not base on act of parliament, but on case of law*, yaitu lewat putusan hakim (*judge made law*). Baca Steven Vago, *Law And Society* (New Jersey : Prentice Hall Inc.,1994), hal.10-11.

1) adanya suatu penawaran *(offer)* dari pihak *offeror* sebagai pihak pertama;
2) adanya penyampaian penawaran tersebut kepada *offeree* sebagai pihak kedua;
3) adanya penerimaan penawaran oleh pihak kedua yang menyatakan kehendaknya untuk terikat pada persyaratan dalam penawaran tersebut;
4) adanya penyampaian penerimaan *(acceptance)* oleh pihak kedua kepada pihak pertama.

Para pihak dalam kontrak harus menunjukkan (baik dengan kata-kata maupun dengan tindakan) kehendak (*intention*) mereka untuk membentuk suatu kontrak. Biasanya dilakukan dengan cara salah satu pihak menyampaikan penawaran (*offer*) dan pihak yang lain menerima penawaran. Dapat ditegaskan bahwa terbentuknya kontrak, terlebih dahulu para pihak yang berkontrak harus memberikan indikasi yang jelas, untuk terikat kontrak, yaitu melalui penawaran dan penerimaan penawaran. Intinya adalah dengan nyata menegaskan penawaran harus dinyatakan dalam bentuk tertentu[27].

Gambar.2.1.

Pihak-Pihak Dalam Suatu Kontrak[28]



[27] M. Arsyad Sanusi, *Konvergensi Hukum dan Teknologi Informasi (Sebuah Torehan Empiris – Yuridis)* (Jakarta : The Indonesian Rearch, 2007), hal. 178-179.

Namun demikian ada tiga syarat yang harus dipenuhi oleh suatu penawaran, yaitu: (a) harus merupakan perwujudan dari kehendak untuk memasuki kontrak; (b) harus disampaikan atau dikomunikasikan kepada pihak lain, dan; (c) harus jelas dan pasti. Selengkapnya dapat dibaca dalam G.H. Treitel, *Treitel on The Law of Contract*, ninth ed. (London : Sweet & Maxwell Limited, 1995).

[28] Gambar dari Soedjono Dirdjosisworo, *Kontrak Bisnis (Menurut Sistem Civil Law, Common Law, dan Praktek Dagang Internasional)* (Bandung: Mandar Maju,2003), hal. 30.

b. Prestasi/*consideration ("something of value"* yang dipertukarkan antara para pihak).

Suatu janji tanpa *consideration* tidak mengikat para pihak dan tidak dapat dituntut pelaksanannya. Dalam sistem *common law*, suatu janji untuk memberikan sesuatu secara cuma-cuma, seperti hibah, tidak mengikat karena tidak ada *consideration.*

> *Consideration is something be given in return, consideration can be viewed as counter promise, price, or action*[29].

Jadi *consideration* adalah suatu kontra prestasi, yang berupa janji, harga atau perbuatan.

c. Kecakapan untuk membuat perjanjian/*capacity*

Pihak-pihak dalam suatu kontrak harus memiliki kapasitas atau kemampuan untuk mengadakan kontrak. Pihak-pihak tertentu, seperti orang-orang yang dianggap kurang akal atau idiot, boros dan di bawah pengampuan, tidak memiliki kemampuan atau kapasitas untuk mengadakan kontrak.

d. Suatu objek yang halal/ *that performance under the contract is legal*[30].

Obyek kontrak haruslah sah atau tidak melawan hukum. Kontrak yang diadakan untuk mencapai tujuan-tujuan atau obyek illegal, atau kontrak-kontrak yang berlawanan atau bertentangan dengan kebijaksanaan pemerintah menjadi batal.

Menurut *common law system*, sebuah kontrak merupakan persetujuan yang mengikat secara hukum (*a legally binding agreement*). Agar sebuah kontrak mengikat secara hukum, proses penawaran dan penerimaan (*offer and acceptance*) yang mengawali penutupan kontrak tersebut harus memenuhi persyaratan tertentu, sebagai berikut :

---

[29] Paul Latimer, *Australian Business Law* (Sydney : CCH Australia Limited, 1998), hal. 271.

[30] David L Baumer dan J.C. Poindexter, *Cyberlaw & E-Commerce* (New York : McGraw-Hill, 2002), hal. 24. Lihat juga di Roy J.Firasa, *Cyberlaw : National And International Perspectives* (New Jersey : Prentice Hall, 2002), hal. 52.

a. Persetujuan *(agreement)* sebagai hasil perundingan para pihak belum menghasilkan perjanjian. Persetujuan hanya menunjukkan adanya persesuaian kehendak *(meeting of minds/consensus ad idem)* dari para pihak tentang beberapa hal;

b. untuk kepentingan hukum, persesuaian kehendak saja tidak cukup, tetapi harus dinyatakan melalui pernyataan (*words*) atau perbuatan *(actions/conduct);*

c. agar penawaran *(offer),* sebagai pernyataan atau perbuatan, mengikat secara hukum *(legally binding),* penawaran tersebut harus jelas, tegas, dan konkrit (*an offer must be clear and unequivocal);*

d. apabila persyaratan ini belum terpenuhi, maka penawaran (*offer*) hanya dipandang sebagai *invitations to treat.*

Persyaratan penawaran *(offer)* yang mendahului kontrak sebagaimana dikemukakan di atas, menyebabkan penawaran di dalam *common law system* senantiasa dilakukan sedemikian rinci sehingga penawaran tersebut jelas,tegas, dan kongkrit. Karakter tingkat kerincian penawaran tidak ditemukan di dalam Buku III KUH Perdata yang merupakan hukum kontrak yang berasal dari rumpun *civil law system.* Karakter tingkat kerincian yang tinggi inilah yang menyebabkan secara fisik kontrak di dalam *common law system* memiliki ketebalan melebihi kontrak di dalam *civil law system,* karena bila kemudian penawaran *(offer)* yang mensyaratkan tingkat kerincian yang tinggi tersebut diterima *(accepted)* oleh penutup kontrak, maka rincian penawaran tersebut akan menjadi ketentuan dan persyaratan *(terms and conditions)* di dalam kontrak yang terjadi[31].

[31] Johannes Gunawan, *Reorientasi Hukum Kontrak Di Indonesia* dalam Jurnal Hukum Bisnis, Volume 22, No.6., (Jakarta : Yayasan Pengembangan Hukum Bisnis, 2003),hal. 46-47.

2.1.2. Kontrak menurut *Civil law* atau *Eropa Kontinental*[32]

Kebanyakan negara yang tidak menerapkan *common law* memiliki sistem *civil law. Civil law* ditandai oleh kumpulan perundang-undangan yang menyeluruh dan sistematis, yang dikenal sebagai hukum yang mengatur hampir semua aspek kehidupan.

Teori mengatakan bahwa *civil law* berpusat pada undang-undang dan peraturan. Undang-Undang menjadi pusat utama dari *civil law*, atau dianggap sebagai jantung *civil law*. Namun dalam perkembangannya *civil law* juga telah menjadikan putusan pengadilan sebagai sumber hukum.

Kontrak menurut civil law akan menggunakan peraturan mengenai perjanjian di Indonesia, yang akan dibahas di bawah ini.

2.1.3. Tinjauan umum tentang perjanjian di Indonesia

Indonesia sebagai akibat 350 tahun dijajah oleh Belanda, merupakan negara yang dipengaruhi sistem *civil law*. Hukum Perikatan di Indonesia diatur secara umum di dalam Buku III Kitab Undang-undang Hukum Perdata tentang Perikatan[33].

---

[32] Sistem hukum Eropa Kontinental adalah suatu sistem hukum dengan ciri-ciri adanya berbagai ketentuan-ketentuan hukum dikodifikasi (dihimpun) secara sistematis yang akan ditafsirkan lebih lanjut oleh hakim dalam penerapannya. Hampir 60% dari populasi dunia tinggal di negara yang menganut sistem hukum ini.

Dapat dilihat di *http://id.wikipedia.org/wiki/Hukum*

[33] Indonesia merupakan negara bekas jajahan Belanda , maka KUHPdt. Belanda diusahakan supaya dapat berlaku pula di wilayah Hindia Belanda. Caranya ialah dibentuk B.W. Hindia Belanda yang susunan dan isinya serupa dengan BW Belanda. Untuk kodifikasi KUHPdt. di Indonesia dibentuk sebuah panitia yang diketuai oleh Mr. C.J. Scholten van Oud Haarlem. Kodifikasi yang dihasilkan diharapkan memiliki kesesuaian antara hukum dan keadaan di Indonesia dengan hukum dan keadaan di negeri Belanda. Di samping telah membentuk panitia, pemerintah Belanda mengangkat pula Mr. C.C. Hagemann sebagai ketua Mahkamah Agung di Hindia Belanda (*Hooggerechtshof*) yang diberi tugas istimewa untuk turut mempersiapkan kodifikasi di Indonesia. Mr. C.C. Hagemann dalam hal tidak berhasil, sehingga tahun 1836 ditarik kembali ke negeri Belanda. Kedudukannya sebagai ketua Mahkamah Agung di Indonesia diganti oleh Mr.C.J. Scholten van Oud Haarlem.

Pada 31 Oktober 1837, Mr.C.J. Scholten van Oud Haarlem di angkat menjadi ketua panitia kodifikasi dengan Mr. A.A. Van Vloten dan Mr. Meyer masing-masing sebagai anggota. Panitia tersebut juga belum berhasil. Akhirnya dibentuk panitia baru yang diketuai Mr.C.J. Scholten van Oud Haarlem lagi,tetapi anggotanya diganti yaitu Mr. J.Schneither dan Mr. A.J. van Nes. Pada akhirnya panitia inilah yang berhasil mengkodifikasi KUHPdt Indonesia maka KUHPdt. Belanda banyak

Dalam kehidupan sehari-hari, kata "perjanjian" atau "kontrak" sering dipergunakan. Jika mendengar kata "perjanjian" maka yang pertama terlintas dalam pemikiran adalah suatu kewajiban yang harus dilaksanakan dan / atau ada suatu hak yang akan diperoleh.

Pertama-tama, perlu dipahami terlebih dahulu bahwa sebenarnya ada perbedaan antara pengertian tentang "perikatan" ataupun " kontrak" dengan pengertian tentang "perjanjian". Perikatan atau kontrak adalah istilah untuk hubungan hukum antar para pihak, sedangkan perjanjian adalah istilah untuk peristiwa hukum yang melahirkan kontrak tersebut. Berdasarkan Buku III Kitab Undang-undang Hukum Perdata tentang perikatan, dikatakan bahwa sumber perikatan adalah undang-undang, perjanjian dan kebiasaan-kebiasaan yang berkembang di masyarakat.

Perikatan yang lahir karena undang-undang dapat kita lihat dalam pertanggungjawaban hukum yang timbul akibat kealpaan (*negligence*), tanggung jawab produk (*product liability*), tanggung jawab profesional (*professional liability*), dan tanggung jawab terhadap informasi yang berlebihan atau menyesatkan (*misleading information*). Pada esensinya, perikatan berdasarkan Undang-undang

---

menjiwai KUHPdt. Indonesia karena KUHPdt. Belanda dicontoh untuk kodifikasi KUHPdt. Indonesia. Kodifikasi KUHPdt. Indonesia diumumkan pada tanggal 30 April 1847 melalui Staatsblad No. 23 dan berlaku Januari 1948.

Setelah Indonesia Merdeka berdasarkan aturan Pasal 2 aturan peralihan UUD 1945, KUHPdt. Hindia Belanda tetap dinyatakan berlaku sebelum digantikan dengan undang-undang baru berdasarkan Undang – Undang Dasar ini. BW Hindia Belanda disebut juga Kitab Undang – Undang Hukun Perdata Indonesia sebagai induk hukum perdata Indonesia.

Pasal 2 ATURAN PERALIHAN UUD 1945

Segala Badan Negara dan Peraturan yang ada masih langsung berlaku, selama belum diadakan yang baru menurut Undang-undang Dasar ini.

Yang dimaksud dengan Hukum perdata Indonesia adalah hukum perdata yang berlaku bagi seluruh Wilayah di Indonesia. Hukum perdata yang berlaku di Indonesia adalah hukum perdata barat [Belanda] yang pada awalnya berinduk pada Kitab Undang-Undang Hukum Perdata yang aslinya berbahasa Belanda atau dikenal dengan Burgerlijk Wetboek dan biasa disingkat dengan B.W. Sebagaian materi B.W. sudah dicabut berlakunya & sudah diganti dengan Undang-Undang RI misalnya mengenai Perkawinan, Hipotik, Kepailitan, Fidusia sebagai contoh Undang-Undang Perkawinan No.1 tahun 1974, Undang-Undang Pokok Agraria No.5 Tahun 1960.

(Disusun oleh RGS & Mitra terdapat di *http://advokat-rgsmitra.com/* atau *http://www.geocities.com/pengacara_rgs/artikel/resume_singkat_hukum_perdata.html*)

adalah berbicara mengenai hak dan kewajiban warga negara kepada masyarakatnya atau negaranya yang didasarkan atas pemberlakuan suatu undang-undang yang ada.

Bidang Hukum Perjanjian di Indonesia diatur secara umum di dalam Buku III Bab Kedua Kitab Undang-undang Hukum Perdata tentang perikatan-perikatan yang dilahirkan dalam kontrak atau perjanjian. Sedangkan untuk perjanjian yang lebih khusus diatur dalam Bab V sampai dengan Bab XVIII. Yang perlu dicatat di sini adalah keberadaan Buku III dalam Kitab Undang-undang Hukum Perdata bersifat terbuka, yang artinya dimungkinkan adanya jenis-jenis perikatan selain yang diatur dalam Buku III ini. Jenis perikatan yang diatur dalam Buku III disebut Perikatan Nominat, sedangkan yang tidak diatur dalam Buku III disebut Perikatan Nominat.

Pengertian perjanjian dapat diketahui dari Pasal 1313 Kitab Undang-Undang Hukum Perdata, yang berbunyi sebagai berikut: " suatu perjanjian adalah suatu perbuatan dengan mana satu orang atau lebih mengikatkan dirinya terhadap satu orang lain atau lebih."[34] Perjanjian yang dimaksud dalam Pasal 1313 tersebut adalah perjanjian obligatoir atau perjanjian timbal balik di mana satu pihak harus melakukan kewajiban dan pihak lain memperoleh hak. Selain itu, pada prakteknya masyarakat akan menyatakan bahwa suatu perjanjian adalah harus tertulis (*writing*) dan bertanda tangan (*signed*) di atas materai (*duty stamp*) ataupun kertas segel serta harus asli (*original*).

Perjanjian akan menimbulkan suatu perikatan yang di dalam kehidupan sehari-hari sering diwujudkan dengan janji atau kesanggupan yang diucapkan atau ditulis. Hubungan hukum dalam perjanjian bukanlah hubungan hukum yang lahir dengan sendirinya tetapi hubungan itu tercipta karena adanya tindakan hukum yang dilakukan oleh pihak-pihak yang berkeinginan untuk menimbulkan hubungan hukum tersebut.

---

[34] Subekti dan Tjitrosudibio, *Kitab Undang-undang Hukum Perdata*, terjemahan *Burgerlijk Wetboek* (Jakarta: Pradnya Paramita, 2006), Pasal 1313.

Kitab Undang-Undang Hukum Perdata memberikan pengertian mengenai perjanjian tetapi pembuat undang-undang tidak memberikan pengertian mengenai perikatan. Dalam bukunya "Hukum Perjanjian", Subekti mencoba memberikan definisi perikatan sebagai berikut:

> Suatu perikatan adalah suatu perhubungan hukum antara dua orang atau dua pihak, berdasarkan mana pihak yang satu berhak menuntut sesuatu hal dari pihak yang lain dan pihak yang lain berkewajiban untuk memenuhi tuntutan itu[35].

Dari pengertian perjanjian atau perikatan dapat ditarik kesimpulan bahwa perjanjian adalah peristiwa hukum sedangkan perikatan adalah hubungan hukumnya, atau dapat dikatakan bahwa perjanjian adalah salah satu sumber perikatan. Hal ini karena perjanjian berisi ketentuan-ketentuan yang menimbulkan hak dan kewajiban di antara para pihak, sehingga perjanjian yang sah berlaku sebagaimana layaknya undang-undang bagi para pihak yang membuatnya (Pasal 1320 KUHPerdata)[36].

Selanjutnya, perjanjian dapat kita temui dalam bentuk perjanjian tertulis ataupun dapat tidak tertulis yang mencakup janji-janji serta kesanggupan secara lisan, tergantung kepada obyek hukum yang diperjanjikan. Mengenai pengalihan hak terhadap benda tidak bergerak maka secara garis besarnya proses pengalihannya

---

[35] Subekti, *Hukum Perjanjian*, Cet. Ke-20 (Jakarta : PT. Intermasa ,2004),hal. 1.

[36] Imran Nating dalam artikel "Pemahaman Tentang Kontrak (Dimensi Nasional dan Internasional)" di http://www.solusihukum.com/artikel/artikel8.php mengutip Anggiat Simamora, *Legal Drafting : Draft Kontrak* , makalah di sampaikan dalam bimbingan profesi sarjana hukum pertamina, (Jakarta: 2001), hal. 2 bahwa Kontrak dalam bahasa Indonesia sering disebut sebagai "perjanjian". Meskipun demikian, apa yang dalam bahasa Indonesia disebut perjanjian, dalam bahasa Inggris tidak selalu sepadan dengan *contract.* Istilah *contract* digunakan dalam kerangka hukum nasional atau internasional yang bersifat perdata. Dalam kerangka hukum internasional publik, yang kita sebut "perjanjian", dalam bahasa Inggris seringkali disebut *treaty* atau kadang-kadang juga *covenant.* Sejauh yang dapat kita ketahui, tidak pernah ada dua pihak swasta atau lebih membuat *treaty* atau *covenant,* sebaliknya, tidak pernah terekam dua negara yang diwakili oleh pemerintah masing-masing membuat suatu *contract.*

Maka dapat disimpulkan oleh penulis bahwa penggunaan istilah perjanjian dalam tesis ini adalah perjanjian yang dibuat melalui transaksi yang menggunakan sarana elektronik, dimana perjanjian tersebut yang dimaksud dalam UU ITE berada dalam kerangka hukum nasional maupun internasional yang bersifat perdata karena para pihak dalam perjanjian bukan merupakan pemerintah dari suatu negara (*business to business*).

harus dilakukan secara "terang" dan "tunai" dengan kata lain harus dibuat dihadapan pejabat yang berwenang, mekanisme keberadaan haknya juga ditentukan oleh pendaftaran terhadap benda itu dalam peraturan perundang-undangan tertentu. Untuk pengalihan benda yang bergerak maka hal tersebut tidak mutlak diperlukan melainkan dapat dilakukan secara tidak tertulis dan tidak perlu dilakukan dihadapan pejabat yang berwenang, karena keberadaan sifat kepemilikannya adalah tergantung pada penguasaan atas benda tersebut (*Bezit* berlaku sebagai *title* yang sempurna, Pasal 1977 ayat (1) Kitab Undang-undang Hukum Perdata).

Perlu juga diketahui bahwa sifat dan hakekat suatu perjanjian, menurut Peter Knight dan J. Fitzsimons adalah merupakan langkah awal (*starting point*), langkah penentu (*setting point*) dan kerangka kerja (*legal framework*) :

> *"a contract should provide framework for an entire transaction to cover as many circumstances which may arise as possible. No contract can hope to cover all contingencies, but disputes can be largely avoided through well drafted contracts which at least provide for the resolution of issues, even if they can non foresee what those issues might be"*[37].

Selanjutnya, dalam rezim hukum kontrak yang berlaku di luar negeri umumnya dikatakan bahwa yang menjadi obyek perikatan adalah segala sesuatu (produk ataupun jasa) yang disepakati oleh para pihak atau dengan kata lain dikatakan apa yang ditawarkan (*offer*) dan apa yang diterima (*acceptance*) oleh para pihak. Sedangkan di Indonesia, umumnya dikatakan bahwa obyek dari suatu perikatan adalah prestasi, baik barang maupun jasa. Prestasi atas barang adalah menyerahkan barang, sedang prestasi atas jasa adalah melakukan suatu pekerjaan, yang berdasarkan Pasal 1601 Kitab Undang-undang Hukum Perdata dibedakan atas perjanjian jasa sementara, perjanjian perburuhan dan perjanjian pemborongan kerja.

Suatu perjanjian atau persetujuan adalah suatu perbuatan dengan mana satu orang atau lebih mengikatkan dirinya terhadap satu orang lain atau lebih untuk

---

[37] Peter Knight, J. Fitzsimons, *Legal Environment of Computing*,(Australia: Addison-Wesley Longman Inc., 1991) dalam Edmon Makarim, *Pengantar Hukum Telematika (suatu kompilasi kajian)*,(Jakarta : PT RajaGrafindo Persada,2005),hal.249.

melakukan sesuatu hal yang telah disepakati oleh para pihak[38]. Dari definisi tersebut dapat ditarik kesimpulan bahwa unsur-unsur dari perjanjian atau persetujuan terdiri dari :

a. Suatu perbuatan

Maksud dari perbuatan disini, sudah pasti adalah perbuatan yang halal, yang tidak bertentangan dengan peraturan perundang-undangan yang berlaku, kesusilaan dan ketertiban umum. Jika ditinjau dari segi pelaksanaan perjanjian, maka perbuatan itu dibagi dalam tiga macam, yaitu :

1) Untuk memberikan atau menyerahkan sesuatu;

Contohnya dalam perjanjian jual beli, pada saat terjadi kesepakatan antara penjual dan pembeli, si penjual wajib untuk menyerahkan benda yang menjadi obyek dalam perjanjian tersebut setelah si pembeli membayar harga yang sesuai dengan kesepakatan awalnya.

2) Untuk berbuat sesuatu;

Contoh konkritnya adalah dalam perjanjian pemborongan, dimana si pemilik rumah membayar sejumlah uang kepada si pemborong untuk membangun atau merenovasi rumahnya.

3) Untuk tidak berbuat sesuatu.[39]

Dalam hal ini, kita bisa mengambil contoh dari sebuah perusahaan yang tidak diperbolehkan meniru atau memperbanyak sebuah produk yang sama, yang telah dipatenkan terlebih dahulu oleh perusahaan yang lain.

b. Terdiri dari dua orang atau lebih

Dalam setiap perjanjian biasanya satu pihak berjanji kepada pihak yang lain atau masing-masing pihak sama-sama berjanji untuk melaksanakan sesuatu, oleh karena itu, tidak mungkin ada perjanjian jika hanya terdiri dari

---

[38] Lihat R.Setiawan, *op.cit.*, hal.49.

[39] Subekti dan Tjitrosudibio, *op.cit.*, Pasal 1234

satu orang saja. Perjanjian selalu menimbulkan hak dan kewajiban yang harus dilaksanakan oleh masing-masing pihak secara timbal balik.

Dalam praktek sehari-hari, perjanjian itu dibuat dalam bentuk rangkaian kata-kata yang mengandung adanya suatu janji atau kesanggupan yang dibuat secara tertulis atau diucapkan secara lisan oleh para pihak.Dari adanya perjanjian yang dibuat oleh para pihak tersebut, timbullah suatu perikatan, yaitu hubungan hukum antara para pihak yang melakukan perjanjian, dimana pihak yang satu dapat menuntut haknya dari pihak yang lain, dan pihak yang lain mempunyai kewajiban untuk memenuhi tuntutan tersebut. Hubungan yang asli bersifat hubungan keluarga tidak termasuk dalam pengertian perikatan seperti kewajiban untuk selalu saling setia dari suami dan isteri[40].

Pada dasarnya suatu perjanjian harus memuat beberapa unsur perjanjian yaitu[41]:

a. unsur *esensialia*, sebagai unsur pokok yang wajib ada dalam perjanjian, seperti identitas para pihak yang harus dicantumkan dalam suatu perjanjian, termasuk perjanjian yang dilakukan jual beli secara elektronik[42].
b. unsur *naturalia*, merupakan unsur yang dianggap ada dalam perjanjian walaupun tidak dituangkan secara tegas dalam perjanjian, seperti itikad baik dari masing-masing pihak dalam perjanjian[43].
c. unsur *aksidentalia*, yaitu unsur tambahan yang diberikan oleh para pihak dalam perjanjian, seperti klausula tambahan yang berbunyi "barang yang sudah dibeli tidak dapat dikembalikan"[44].

---

[40] Tommy M. Kleian dan Humphrey R. Djemat, *Compendium Hukum Perikatan* (Jakarta: Indonesia Bussiness Law Center, 2006), hal. 19.

[41] Subekti, *Aneka Perjanjian*, Cet.VII, (Bandung : Alumni, 1985), hal. 20.

[42] Lihat juga Kartini Muljadi dan Gunawan Widjaja, *Perikatan Yang Lahir dari Perjanjian* (Jakarta:PT RajaGrafindo Persada,2006), hal. 86.

[43] *Ibid.*, hal.88.

[44] *Ibid.*, hal.89.

Dalam suatu perjanjian harus diperhatikan pula beberapa macam azas yang dapat diterapkan antara lain[45] :

a. Azas Konsensualisme, yaitu azas kesepakatan, dimana suatu perjanjian dianggap ada seketika setelah ada kata sepakat.

b. Azas Kepercayaan, yang harus ditanamkan diantara para pihak yang membuat perjanjian.

c. Azas kekuatan mengikat, maksudnya bahwa para pihak yang membuat perjanjian terikat pada seluruh isi perjanjian dan kepatutan yang berlaku.

d. Azas Persamaan Hukum, yaitu bahwa setiap orang dalam hal ini para pihak mempunyai kedudukan yang sama dalam hukum.

e. Azas Keseimbangan, maksudnya bahwa dalam melaksanakan perjanjian harus ada keseimbangan hak dan kewajiban dari masing-masing pihak sesuai dengan apa yang diperjanjikan.

f. Azas Moral adalah sikap moral yang baik harus menjadi motivasi para pihak yang membuat dan melaksanakan perjanjian.

g. Azas Kepastian Hukum yaitu perjanjian yang dibuat oleh para pihak berlaku sebagai undang-undang bagi para pembuatnya.

h. Azas Kepatutan maksudnya bahwa isi perjanjian tidak hanya harus sesuai dengan peraturan perundang-undangan yang berlaku tetapi juga harus sesuai dengan kepatutan, sebagaimana ketentuan Pasal 1339 KUH Perdata yang menyatakan bahwa suatu perjanjian tidak hanya mengikat untuk hal-hal yang dengan tegas dinyatakan didalamnya, tetapi juga untuk segala sesuatu yang menurut sifat perjanjian diharuskan oleh kepatutan, kebiasaan atau undang-undang.

i. Azas Kebiasaan, maksudnya bahwa perjanjian harus mengikuti kebiasaan yang lazim dilakukan, sesuai dengan isi Pasal 1347 KUH Perdata yang berbunyi hal-

---

[45] Tim Naskah Akademis BPHN, *Naskah Akademis Lokakarya Hukum Perikatan*, (Jakarta: Badan Pembinaan Hukum Nasional, 1985) dalam Lokakarya Hukum Perikatan yang diselenggarakan oleh Badan Pembinaan Hukum Nasional (BPHN), Departemen Kehakiman RI pada tanggal 17 – 19 Desember 1985.

hal yang menurut kebiasaan selamanya diperjanjikan dianggap secara diam-diam dimasukkan ke dalam perjanjian, meskipun tidak dengan tegas dinyatakan. Hal ini merupakan perwujudan dari unsur naturalia dalam perjanjian.

Semua ketentuan perjanjian tersebut diatas dapat diterapkan pula pada perjanjian yang dilakukan melalui media internet, seperti perjanjian jual beli secara elektronik, sebagai akibat adanya perkembangan ilmu pengetahuan dan teknologi.

Untuk menentukan sahnya suatu perjanjian, harus memenuhi ketentuan-ketentuan yang terdapat pada Pasal 1320 Kitab Undang-undang Hukum Perdata[46], yaitu :

a. Sepakat mereka yang mengikatkan dirinya ;
Jika tidak ada kesepakatan, maka tidak akan pernah ada perjanjian dari awalnya.

Suatu kesepakatan selalu diawali dengan adanya suatu penawaran oleh suatu pihak dan dilanjutkan dengan adanya tanggapan berupa penerimaan oleh pihak lain. Jika penawaran tersebut tidak ditanggapi atau direspon oleh pihak lain maka dengan demikian tidak akan ada kesepakatan. Karena itu diperlukan dua pihak untuk melahirkan suatu kesepakatan.

Pada perjanjian jual beli secara langsung, kesepakatan dapat dengan mudah diketahui. Sebab kesepakatan dapat langsung diberikan secara lisan maupun tulisan. Tetapi dalam transaksi melalui *e-commerce,* kesepakatan dalam perjanjian tersebut tidak diberikan secara langsung melainkan melalui media elektronik dalam hal ini adalah internet.

Dalam transaksi *e-commerce,* pihak yang memberikan penawaran adalah pihak penjual yang dalam hal ini menawarkan barang-barang dagangannya melalui *website* yang dirancang agar menarik untuk disinggahi. Semua pihak pengguna

[46] Subekti dan Tjitrosudibio, *op.cit.*, Pasal 1320

internet *(netter)* dapat dengan bebas masuk untuk melihat-lihat toko *virtual* tersebut atau untuk membeli barang yang mereka butuhkan atau minati.

Jika memang pembeli tertarik untuk membeli suatu barang maka ia hanya perlu mengklik barang yang sesuai dengan keinginannya. Biasanya setelah pesanan tersebut sampai di tempat penjual *(merchant]* maka penjual *(merchant)* akan mengirim *e-mail* atau melalui telepon untuk mengkonfirmasi pesanan tersebut kepada konsumen.

Proses terciptanya penawaran dan penerimaan tersebut menimbulkan keraguraguan kapan terciptanya suatu kesepakatan. Negara-negara yang tergabung dalam Uni Eropa telah memberikan garis-garis petunjuk kepada para negara anggotanya, dengan memberlakukan sistem "3 klik"[47].

> Cara kerja sistem ini adalah: Pertama, setelah calon pembeli melihat di layar komputer adanya penawaran dari calon penjual (klik pertama), maka si calon pembeli memberikan penerimaan terhadap penawaran tersebut (klik kedua). Dan masih disyaratkan adanya peneguhan dan persetujuan dari calon penjual kepada pembeli perihal diterimanya penerimaan dari calon pembeli (klik ketiga). Sistem tiga klik ini jauh lebih aman daripada sistem 2 klik yang berlaku sebelumnya. Sebab dalam sistem "2 klik", penjual dapat mengelak dengan menyatakan kepada calon pembeli bahwa ia tidak pernah menerima "penerimaan" dari calon pembeli. Dan ini tentunya akan merugikan pembeli[48].

Dalam hukum Indonesia sebelum diundangkannya UU ITE belum ada ketentuan semacam ini, tidak ada kewajiban dari penjual untuk melakukan konfirmasi kepada pembeli, sehingga banyak penjual yang tidak melakukan konfirmasi. Hal ini sangat merugikan konsumen/pembeli karena pembeli tidak mengetahui apakah pesanannya telah diterima atau belum. Jika terjadi wanprestasi akan sulit menghitung kapan terjadinya wanprestasi karena penjual

---

[47] Edmon Makarim dan Deliana, "Kajian Aspek Hukum Perikatan" dalam Edmon Makarim, *Kompilasi Hukum Telematika* (Jakarta : PT RajaGrafindo Persada, 2003), hal. 234-235.

[48] *Ibid.* mengutip Setiawan, "Electronic Commerce : Tinjauan dari Segi Hukum Kontrak," (Makalah disampaikan pada Seminar *Legal Aspects of E-commerce*, Jakarta, Agustus 2000), hal.4.

(merchant) dapat dengan mudah mendalilkan bahwa ia tidak menerima pesanan tersebut. Dalam Pasal 20 UU ITE diatur bahwa transaksi elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima, kecuali ditentukan lain oleh para pihak dan persetujuan atas penawaran transaksi elektronik harus dilakukan dengan pernyataan penerimaan secara elektronik.

b. Kecakapan untuk membuat suatu perikatan ;

Batasan dari seseorang dikatakan cakap adalah sudah dewasa, dalam hal ini sudah berusia 21 tahun atau sudah pernah menikah, tidak ditaruh di bawah pengampuan dan mempunyai akal yang sehat. Bagi orang-orang tertentu yang ingin melakukan perjanjian tapi tidak memenuhi syarat kecakapan ini, harus didampingi dengan orang-orang yang dianggap berkompeten untuk melakukan tindakan hukum atas nama mereka, seperti contohnya untuk anak yang masih dibawah umur jika ingin membuat suatu perjanjian, harus didampingi dengan orangtuanya. Begitu juga dengan orang yang ditaruh di bawah pengampuan, jika ia ingin mengikatkan dirinya dalam suatu perjanjian juga harus dengan bantuan pengampunya.

Dalam transaksi *electronic commerce* sangat sulit menentukan seseorang yang melakukan transaksi telah dewasa atau tidak berada di bawah pengampuan, karena proses penawaran dan penerimaan tidak secara langsung dilakukan tetapi hanya melalui media *virtual* yang rawan penipuan[49].

c. Suatu hal / obyek yang tertentu ;

Obyek dalam suatu perjanjian harus dijelaskan secara khusus dan terperinci, agar mempermudah pelaksanaan dari perjanjian.

d. Suatu sebab yang halal (*a premissible cause*)

---

[49] *Ibid.*,hal.236.

Suatu perjanjian harus dibuat berdasarkan adanya suatu maksud atau tujuan dari para pihak yang tidak bertentangan dengan peraturan perundang-undangan yang berlaku, kesusilaan dan ketertiban umum.

Syarat pertama dan kedua adalah mengenai subyeknya atau pihak-pihak dalam perjanjian, sehingga disebut sebagai syarat subyektif, sedangkan syarat ketiga dan keempat disebut syarat obyektif karena mengenai benda atau obyek dalam suatu perjanjian.

Adanya syarat subyektif dan syarat obyektif sebagai syarat sahnya perjanjian harus dibedakan. Jika syarat subyektif tidak dapat terpenuhi, maka salah satu pihak mempunyai hak untuk meminta agar perjanjian itu dibatalkan. Pihak yang dapat meminta pembatalan adalah pihak yang tidak cakap atau pihak yang memberikan kata sepakatnya dengan cara yang tidak bebas[50]. Dalam hal yang melakukan tindakan hukum tersebut adalah seorang anak yang masih di bawah umur, maka yang dapat meminta pembatalan adalah anak sendiri tersebut jika ia sudah dewasa, akan tetapi dalam hal yang melakukan tindakan hukum tersebut adalah seseorang yang ditaruh dibawah pengampuan, maka yang dapat meminta pembatalannya adalah si pengampunya. Bila syarat obyektif yang tidak terpenuhi, maka perjanjian itu batal demi hukum. Artinya, perjanjian itu dianggap tidak pernah ada, sehingga tidak pernah ada perikatan yang lahir dari para pihak. Dengan demikian para pihak tidak bisa saling menuntut di hadapan hakim, karena tidak adanya alasan yang kuat, dalam hal ini perjanjian diantara mereka tidak pernah terjadi.

[50] Subekti, *Hukum Perjanjian,* Cet.Ke-20,(Jakarta : PT. Intermasa, 2004), hal.20.

2.2. TINJAUAN UMUM TENTANG PERJANJIAN DALAM TRANSAKSI ELEKTRONIK

2.2.1. Pengertian *E-Commerce*

Dalam *United Nations Commission on International Trade (UNCITRAL) Model Law On Electronic Commerce with Guide to Enactment 1996*[51] dinyatakan bahwa :

> *The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road*[52].

Berdasarkan ruang lingkupnya, maka dalam praktek bisnis yang berkembang berdasarkan lingkup aktifitasnya, dikenal juga pembedaan sebagai berikut :

a. *Electronic Business* adalah ditujukan untuk lingkup aktivitas perdangan dalam arti luas;
b. *Electronic Commerce* adalah ditujukan untuk lingkup perdagangan/perniagaan yang dilakukan secara elektronik dalam arti sempit, termasuk[53];
   1) Perdagangan via Internet (*Internet Commerce*);

---

[51] *In 1996, UNCITRAL drafted the UNCITRAL Model Law on E-Commerce in order to assist countries in enacting laws to enable electronic contracting. The UNCITRAL Model Law on E-Commerce extends the scope of the national legal definitions of "writings", "signatures", and "originals" to cover electronic signatures and records. The UNCITRAL Model Law on E-Commerce has been influential among the drafters of national electronic transaction legislation. It has served both to educate lawmakers about the legal ramifications of electronic transactions and as a framework for countries wishing to draft electronic transaction legislation.*

[52] http://www.law.upenn.edu/bll/archives/ulc/uecicta/ecomemo.txt

[53] Lihat juga Mieke Komar Kantaatmadja, "Pengaturan Kontrak Untuk Perdagangan Elektronik (E-Contracts)" dalam *Cyberlaw : Suatu Pengantar*, (Bandung : ELIPS II,2002), hal. 2.

2) Perdagangan dengan fasilitas Web Internet (*Web Commerce*) dan

3) Perdagangan dengan Sistem Pertukaran Data terstruktur Secara Elektronik (*Electronic Data Interchange*).

Meskipun istilah *e-commerce* memang baru saja muncul di Indonesia tetapi sebenarnya *e-commerce* telah muncul dengan bentuknya yang beraneka ragam sejak dua puluh tahun terakhir, seiring dengan semakin populernya teknologi *Electronic Data Interchange* (EDI) dan *Electronic Funds Transfer* (EFT) diperkenalkan pertama kalinya di akhir tahun 1970-an. Pertumbuhan penggunaan *Credit Cards, Automated Teller Machines* dan *Telephone Banking* diperkenalkan tahun 1980-an[54]. Dengan demikian dapat dikatakan hanya istilahnya saja yang baru dipakai, padahal sebenarnya masyarakat telah mengenal *e-commerce* bahkan telah melakukan transaksi *e-commerce* itu sendiri.

E-commerce (perdagangan secara elektronik) menurut Julian Ding adalah transaksi dagang antara penjual dengan pembeli untuk menyediakan barang, jasa, atau mengambil alih hak. Kontrak ini dilakukan dengan media elektronik dimana para pihak tidak hadir secara fisik. Media ini terdapat di dalam jaringan umum dengan sistem terbuka yaitu internet atau world wide web, transaksi ini terjadi terlepas dari batas wilayah dan syarat nasional, karena terjadi di dunia maya[55].

Transaksi *e-commerce* berbeda dengan transaksi perdagangan pada umumnya. *E-Commerce* memiliki beberapa karakteristik khusus yaitu:

a. Transaksi tanpa batas: dengan menggunakan internet, tidak ada lagi batas-batas geografi menjadi penghalang untuk bertransaksi. Semua perusahaan baik itu besar ataupun kecil dapat bertransaksi secara internasional. Cukup dengan membuat situs web atau dengan memasang iklan di situs-situs internet tanpa

---

[54] Sutan Remy Sjahdeini, *E-Commerce Tinjauan Dari Perspektif Hukum* dalam Jurnal Hukum Bisnis, Volume 12, (Jakarta : Yayasan Pengembangan Hukum Bisnis,2001), hal.17.

[55] Terjemahan bebas definisi *e-commerce* dalam Julian Ding, *E-commerce: Law & Practice*, (Kuala Lumpur : Sweet&Maxwell,1999), hal.25.

batas waktu, seluruh pelanggan dari seluruh dunia dapat mengakses dan bertransaksi secara *on-line*.

b. Transaksi anonim: para penjual dan pembeli pun tidak harus bertemu muka secara langsung (*faceless nature*). Penjual tidak memerlukan nama pembeli sepanjang proses pembayaran telah diotorisasi oleh pihak penyedia sistem pembayaran, biasanya kartu kredit.

c. Produk digital dan non digital: produk digital seperti *software*, musik, dan produk lain yang bersifat digital dapat ditransaksikan dengan cara men*download* secara elektronik. Pada saat ini tidak hanya produk digital saja, kebutuhan-kebutuhan lainnya pun sudah mulai ditransaksikan melalui *e-commerce*.

d. Produk barang tak berwujud : banyak perusahaan yang bergerak di bidang *e-commerce* menawarkan barang tak berwujud separti data, software dan ide-ide yang dijual melalui internet[56].

2.2.2. Pengaturan Kontrak *E-Commerce* Dalam Konvensi Internasional

Kontrak berdasarkan *United Nations Convention in Contracts for International Sale of Goods* (UNCISG)[57]

Kontrak perdagangan internasional secara umum (bukan dalam konteks *e-commerce*) diatur dalam *United Nations in Contracts for International Sale of Goods* (UNCISG) 1980 dan 1986. Indonesia belum meratifikasi untuk UNCISG tahun 1980, meskipun demikian konvensi ini patut kita pertimbangkan sebagai *platform* bagi

---

[56] *http://209.85.175.104/search?q=cache:_8ROLMFajDEJ:elearning.unej.ac.id/courses/KD225/work/466f560f31aceMengenal_E-com.doc+mengenal+ecommerce&hl=en&ct=clnk&cd=1*

[57] Andiono, dkk. *Tinjauan Kritis Atas CA (Certificate/Certification Authority) RUU ITE dalam Prespektif Akademis*, dapat dibaca selengkapnya di http://209.85.175.104/search?q=cache:leWIbdXXpc4J:www.mti.ugm.ac.id/~slamet/kuliah/Aspek_Legal/uu/tugas%2520pak%2520ongkokel%25205/Tugas%2520Aspek%2520Legal%2520-%2520Tinjauan%2520kritis%2520RUU%2520ITE%2520CA.doc+pengaturan+certification+authority+di+amerika&hl=id&ct=clnk&cd=4&gl=id

konvensi jual beli internasional yang baru. Konvensi ini mengatur masalah-masalah kontraktual yang berhubungan dengan kontrak jual beli internasional.

Konvensi ini sebenarnya hanya mengatur masalah jual beli antara *business to business* (B2B), sedangkan *e-commerce* yang kita bahas disini adalah hubungan bisnis antara *Business to Consumer* (B2C) dan juga *business to business* tetapi di dalam konvensi tersebut terdapat beberapa prinsip yang dapat diadopsi. Konsepsi yang bisa diambil dari konvensi ini antara lain adalah:

a. Bahwa kontrak tidak harus dalam bentuk tertulis (*in writing from*), tetapi kontrak tersebut bisa saja berbentuk lain bahkan hanya berdasarkan saksi. Berdasarkan aturan tersebut suatu kontrak dapat juga dalam bentuk data elektronik (misalnya dalam format *data form* yang di-*sign* dengan *digital signature*) tapi didalam UNCISG ini belum diatur secara spesifik mengenai *digital signature*. Berdasarkan hal tersebut diatas maka suatu kontrak jual-beli secara internasional yang menggunakan *digital signature* berdasarkan hukum internasional secara hukum mengikat (*legally binding*) atau mempunyai kekuatan hukum. Mengenai sahnya suatu kontrak yang berbentuk *digital signature* ini sebaiknya diatur dalam perundang-undangan tersendiri seperti seperti halnya yang dilakukan di Amerika Serikat (negara bagian Utah, California), Malaysia, Singapura.
b. CISG mencakup materi pembentukan kontrak secara internasional yang bertujuan meniadakan keperluan menunjukkan hukum negara tertentu dalam kontrak perdagangan internasional serta untuk memudahkan para pihak dalam hal terjadi konflik antar sistem hukum. CISG berlaku terhadap kontrak untuk pejualan barang yang dibuat diantara pihak yang tempat dagangnya berada di negara yang berlainan Pasal (1(1)). Dengan demikian yang menentukan adalah tempat perdagangannya dan bukan kewarganegaraannya. Dalam konteks *digital signature* tempat kedudukan dari *Merchant* yang adalah kedudukan hukum yang tercantum di *digital certificate* miliknya. Suatu kontrak yang dibuat berdasarkan CISG (misalnya berupa *digital signature*) atau yang tunduk

kepada CISG harus ditafsirkan berdasarkan prinsip-prinsip yang tercantum dalam CISG dan kalau CISG belum menentukan, berdasarkan kaaidah-kaidah hukum perdata internasional. Disamping itu, CISG menerima kebiasaan dagang serta kebiasaan antara para pihak sebagai dasar penafsiran ketentuan kontrak. Seperti halnya dalam hukum kontrak Indonesia, itikad baik dijadikan prinsip utama dalam penaafsiran utama dalam penafsiran ketentuan dan pelaksanaan kontrak. Berdasarkan hal-hal tersebut diatas maka hendaknya setiap bentuk kontrak perdagangan internasional dengan menggunakan *digital signature* selain didasarkan pada peraturan yang mengatur secara spesifik mengatur tentang *digital signature* juga didasarkan pada UNCISG karena CISG banyak dipakai oleh negara-negara di dunia.

c. Saat terbentuknya kontrak, ini menyangkut kapan terjadinya kesepakatan terutama apabila kesepakatan ini terjadi tanpa kehadiran para peserta/pihak. Transaksi di internet kita analogikan sebagai transaksi yang dilakukan tanpa kehadiran para pelaku di satu tempat (*between absent person*). CISG memberikan kepastian di dunia perdagangan internasional mengenai saat terjadinya suatu kontrak. Kepastian ini akan memberikan dalam *e-commerce* tanpa adanya kepastian ini, pertukaran antara suatu *digital signature* akan sulit menimbulkan hak dan kewajiban yang diakui oleh hukum kontrak. E-mail meskipun sifatnya menghubungkan para pihak dengan hampir seketika tetapi tetap saja terjadi keterlambatan (*delay*) dalam masalah transmisinya. Juga harus dipertimbangkan adanya sistem yang tidak bekerja secara sempurna sehingga suatu *offer/acceptance* tidak dapat diterima secara seketika. Kontrak jual-beli dianggap sudah ada setelah adanya kesepakatan yang datang dari keduabelah pihak (lihat diatas cara melakukan *offer*).

Kontrak berdasarkan UNCITRAL *Model Law on Electronic Commerce*

Electronic commerce secara internasional sudah diatur oleh *United Nations Commission on International Trade (UNCITRAL)* dalam *UNCITRAL Model Law On Electronic Commerce with Guide to Enactment 1996*[58].

Model law ini mengatur tentang *e-commerce* secara umum, mulai dari definisi-definisi yang dipakai, bentuk dokumen-dokumen yang dipakai dalam *e-commerce*, keabsahan kontrak, saat terjadinya kontrak selain itu *model law* ini mengatur juga tentang *carriage of goods*.

Beberapa hal yang perlu digarisbawahi *Law on Electronic Commerce* 1996 seperti yang dikutip dari *US Framework for Global Electronic Commerce 1997* adalah

> "*Internationally, the United Nations Commision on International Trade Law (UNCITRAL) , has completed work on a model law that supports the commercial used of internatonal contracts in electronic commerce . This model law establishes rules and norms that validate and recognize contract fromed through electronic means , sets default rules for contract formation and governance of electronic contract performance, defines the characteristicof a valid electronic writing and an original document ,provides far the acceptability of electronic signatures for legal and commercial purposes and support the admission of computer evidence in court and arbitration proceedings* "[59]

Dari uraian kutipan tersebut terdapat penekanan pada *validity and recoqnition of electronic contract performance* (keabsahan serta pengakuan diambil beberapa *issues* terhadap bentuk kontrak elektronis) dimana dapat[60], yaitu :

a. *Writing required* (tulisan yang dikehendaki atau dibutuhkan)

---

[58] dengan tambahan Pasal 5 bis yang diadopsi tahun 1998.

[59] UNCITRAL Model Law EC, 1996, hal.3.

[60] Richard Hill dan Ian Walden, *The Draft UNCITRAL Model Law for Electronic Commerce:Issues and Solutions (Teaching Materials)*,1996, hal.1.

Bentuk tulisan menurut Pasal 5 dalam model hukum, secara eksplisit memberikan nilai legal yang sama kepada transmisi elektronik seperti halnya bentuk tertulis[61]:

> *"(1) Where a rule of law requires information to be in writing or to be presented in writing, or provides for certain consequences if it is not, a data message satisfies that rule if the information contained therein is accessible so as to be usable for subsequent reference."*

Penyamaan nilai legal antara transmisi elektronik dengan bentuk tertulis ini dimaksudkan untuk mempermudah posisi transmisi ini sehingga dapat digunakan sebagai bukti nyata dalam pembuktian dan sebagai salah satu pendekatan yang relatif paling mudah sebagai solusi yang ditawarkan.

b. *Signature required* (tanda tangan yang dikehendaki)

Tanda tangan dalam model hukum secara eksplisit memberikan solusi teknis yang pas dan sama nilai legalnya dengan tandatangan tradisional, yang dalam maksud-maksud tertentu para pihak bisa menyetujuinya jika mereka mau. Teknologi tandatangan elektronik masa depan 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[62].

Pendekatan yang diambil dalam model law ini adalah bahwa suatu informasi tidak dapat dikatakan tidak mempunyai kekuatan hukum, tidak mempunyai kekuatan hukum, karena informasi itu berbentuk *data message*. Berdasarkan pendekatan diatas maka suatu *data messages* apapun bentuk atau formatnya tidak dapat dikatakan tidak mempunyai kekuatan hukum hanya karena ia berbentuk suatu *data messages*. Pendekatan ini akan menimbulkan suatu kepastian dikemudian hari apabila terdapat suatu bentuk/format *data messages* dalam bentuk yang baru. Pendekatan ini juga akan menyebabkan suatu kontrak/perjanjian yang dibuat dengan *digital signature*

---

[61] Richard Hill dan Ian Walden, *ibid.*,hal.6.

[62] *ibid.*,hal.7.

mempunyai kekuatan hukum. Apabila dalam suatu perundang-undangan terdapat persyaratan bahwa harus dalam bentuk tertulis, maka persyaratan ini dapat dicapai, selama informasi/data tersebut dapat dilihat/diakses. Apabila suatu perundang-undangan menghendaki adanya suatu tandatangan sebagai tanda sahnya suatu dokumen maka hal ini dapat dicapai dengan cara:

a. terdapat suatu metode yang digunakan untuk mengidentifikasi keberadaan seseorang dan juga dapat mengindikasikan didalam dokumen tersebut telah mendapat persetujuan dari orang tersebut.
b. bahwa metode tersebut diatas dapat dipercaya/dapat dipertanggungjawabkan sehingga data tersebut dapat dengan aman disebarluaskan.

Pendekatan tersebut diatas sifatnya adalah sangat luas/tidak jelas. Metode *digital signature* adalah salah satu cara yang dapat mensiasati kebutuhan adanya suatu tandatangan dalam sebuah dokumen.

Beberapa prinsip utama dalam *UNCITRAL Model Law on Electronic Commerce* adalah[63]:

a. Segala informasi elektronik dalam bentuk data elektronik dapat dikatakan memiliki akibat hukum, keabsahan ataupun kekuatan hukum.
b. Dalam hukum mengharuskan adanya suatu informasi dalam bentuk tertulis maka suatu data elektronik dapat memenuhi syarat untuk itu. Hal ini disebutkan dalam Pasal 6 UNCITRAL Model Law.
c. Dalam hal tanda tangan, maka suatu tanda tangan elektronik merupakan dengan tanda tangan yang sah. Transaksi elektronik dapat dilakukan dengan tanda tangan digital atau tanda tangan elektronik. Tanda tangan digital adalah pendekatan yang dilakukan oleh teknologi atau adanya penghubung antara suatu dokumen/data/message dengan orang yang membuat atau menyetujui

[63] Mariam Darus Badrulzaman, *E-Commerce Tinjauan Dari Hukum Kontrak Indonesia* dalam Jurnal Hukum Bisnis, Volume 12, (Jakarta : Yayasan Pengembangan Hukum Bisnis,2001), hal.38. Bandingkan juga dengan Mieke Komar,*ibid.*,hal. 3-4.

dokumen tersebut. Sedangkan tanda tangan elektronik adalah suatu teknik penandatanganan yang menggunakan *biometric* ataupun berbagai cara lainnya, artinya selalu harus menggunakan *public key crypthography*.

d. Dalam hal kekuatan pembuktian dari data bersangkutan, maka *data message* memiliki kekuatan pembuktian.

Berkenaan dengan format dan keabsahan kontrak dalam Bab III Model Law tersebut dikatakan bahwa: "suatu penawaran dan penerimaan tawaran tersebut dapat dinyatakan dalam bentuk *data message*, dan jika data tersebut digunakan sebagai format dari kontrak maka kontrak tersebut tidak dapat ditolak keabsahaannya dan kekuatan hukumnya dalam mana data tersebut digunakan dan dalam hal pihak-pihak yang melakukan *offer* dan *acceptance* dikatakan sebagai *originator* yaitu sebagai pihak yang melakukan suatu pengiriman data dan pihak yang menerima data dikatakan sebagai *addressee*."[64]

Kontrak berdasarkan *United Nations Convention on the Use of Electronic Communications in International Contracts* 2005[65]

Tujuan utama pembentukan konvensi ini adalah menghilangkan ganjalan atas rintangan yang mungkin timbul sehubungan dengan penggunaan komunikasi secara elektronik dalam kontrak internasional. Rintangan yang mungkin timbul adalah instrumen-instrumen hukum yang kemungkinan akan menghambat praktek-praktek perdagangan baru melalui sarana elektronik. Seperti kita maklumi, hukum lahir dan diformalisasikan dalam jangka waktu yang relatif lama, sedangkan praktek dan teknik perdagangan maju dengan sangat cepat.

---

[64] Edmon Makarim, *Kompilasi Hukum Telematika*,(Jakarta:PT RajaGrafindo Persada,2003),hal.225-227.

[65] Disahkan oleh Majelis Umum PBB tanggal 23 November 2005, sampai tanggal 16 Januari 2008 batas penandatanganan terakhir, hanya 18 negara (daftar Negara yang menandatangani dapat dilihat di *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html*)yang menandatangani konvensi tersebut tetapi belum ada yang meratifikasi konvensi tersebut untuk membuat konvensi tersebut berlaku dan mengikat.

Tujuan lainnya adalah agar keberadaan instrumen hukum di bidang komunikasi elektronik, di bidang kontrak ini, diharapkan akan menciptakan kepastian hukum di kalangan dunia usaha. Hal ini dipandang perlu terutama karena kegiatan bisnis mereka sebagian besar dewasa ini sudah mengandalkan atau menggunakan komunikasi secara elektronik sebagai bagian dari kegiatan bisnisnya.

Konvensi mulai dibuka untuk negara-negara yang mau menandatangani atau mengikatkan diri sejak tanggal 16 Januari 2006 hingga 16 Januari 2008. Untuk berlaku Konvensi membutuhkan hanya 3 (tiga) instrumen ratifikasi.

Substansi konvensi[66] :

a. Ruang lingkup berlaku konvensi

Konvensi terdiri dari 4 bab dan 25 Pasal. Substansi konvensi berlaku terbatas pada :

1) Kontrak yang dilakukan dengan menggunakan komunikasi elektronik oleh para pihak yang tempat usahanya berada di negara yang berbeda. Kriteria terbatas ini yang menjadi batasan lingkup berlakunya konvensi. Jadi faktor nasionalitas para pihak, atau bidang atau jenis transaksi daqang atau bentuk kontrak tidak menjadi kriteria atau faktor yang menentukan untuk berlakunya konvensi.

2) Transaksi konsumen atau transaksi untuk keperluan rumah tangga.

3) Transaksi tukar menukar yang terkait dengan kegiatan perbankan (misalnya *foreign exchange transactions,* sistem pembayaran antar bank, kesepakatan pembayaran antar bank, kliring, dan lain-lain).

4) Konvensi tidak juga berlaku terhadap transfer hak-hak jaminan *(security rights),* peralihan utang, jual beli jaminan, dan sejenisnya; dan

---

[66] Huala Adolf, *Dasar-Dasar Hukum Kontrak Internasional*, Cet.Pertama, (Bandung: PT.Refika Aditama, 2007), hal.42-44.

5) Konvensi tidak juga berlaku terhadap transaksi surat berharga *[bills of exchange)*, surat utang *{promissory notes), consignment notes*, surat pengangkutan laut *{bills of lading* atau konosemen) atau dokumen-dokumen dalam pengangkutan barang di laut[67].

b. Prinsip utama yang Konvensi gariskan adalah prinsip otonomi para pihak. Berdasarkan Pasal 3 Konvensi, para pihak bebas untuk tidak menggunakan aturan substansi konvensi.Termasuk di dalamnya adalah kebebasan para pihak untuk membuat peraturan berbeda dalam peraturan nasionalnya.

c. Status hukum komunikasi elektronik

Aturan penting Konvensi adalah mengenai status hukum komunikasi elektronik. Pasal 8 Konvensi menyatakan bahwa suatu komunikasi atau suatu kontrak tidak boleh disangkal keabsahannya atau kekuatan hukumnya *[enforceability)* semata-mata karena komunikasi atau kontrak tersebut dibuat dalam bentuk komunikasi secara elektronik (ayat 1).

Khusus untuk status hukum kontrak, konvensi tidak mensyaratkan suatu bentuk tertentu. Dalam hal ini tampaknya konvensi menahan diri untuk tidak turut campur terhadap urusan tentang persyaratan bentuk dan keabsahan suatu kontrak, termasuk di dalamnya persyaratan tertulis atau persyaratan tanda tangan.

d. Persyaratan formil kontrak

Konvensi tidak menekankan suatu persyaratan formil tertentu untuk keabsahan suatu kontrak. Artinya, Konvensi tidak mensyaratkan suatu bentuk tertentu untuk suatu kontrak. Dalam posisinya tersebut, Konvensi menyadari kemungkinan adanya persyaratan formal tertentu yang diharuskan oleh negara anggota Konvensi, misalnya persyaratan bahwa kontrak harus memenuhi syarat bentuk tertentu seperti kontrak harus tertulis, kontrak harus ditanda-tangani

[67] Pasal 1 *United Nations Convention on the Use of Electronic Communications in International Contracts* 2005

atau kontrak harus dibuat dalam bentuknya yang asli *(original form)*. Berikut adalah jawaban Konvensi terhadap syarat-syarat formil tersebut.

1) Syarat kontrak harus tertulis

Dalam menghadapi persyaratan ini, Konvensi hanya menyatakan bahwa Konvensi tidak mensyaratkan bentuk tertulis ini. Konvensi menegaskan bahwa apabila hukum nasional mensyaratkan hal ini, maka Konvensi menegaskan bahwa kontrak internasional yang dilakukan secara elektronik memenuhi syarat ini. Menurut Konvensi syarat tertulis harus dipandang tidak dipenuhi karena komunikasi secara elektronik dapat diakses kembali atau digunakan kembali sebagai acuan lebih lanjut *('that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference')*.

2) Syarat harus ada tandatangan

Konvensi menegaskan bahwa kontrak internasional yang dilakukan secara elektronik memenuhi syarat tanda-tangan. Menurut Konvensi, syarat tanda tangan harus dipandang dipenuhi apabila :

a) para pihak menggunakan suatu metode tertentu dapat mengenali para pihak dan dapat mengenali kehendak para pihak yang tertuang dalam informasi yang termuat dalam komunikasi elektronik; dan

b) Metode tertentu yang digunakan seperti tersebut dalam (a) di atas dapat diandalkan sebagai metode yang tepat dan metode tersebut memenuhi fungsi sebagai suatu metode tertentu yang dapat dinyatakan dari metode itu sendiri. Metode tersebut dapat pula dipertegas keandalannya oleh bukti-bukti.

3) Bentuk asli kontrak

Dalam hal adanya persyaratan bentuk asli dari suatu kontrak internasional, Konvensi menyatakan bahwa persyaratan tersebut dipenuhi oleh kontrak-kontrak internasional yang dilakukan secara elektronik, dengan bukti sebagai berikut :

a) bahwa kontrak secara elektronik memiliki jaminan yang dapat diandalkan mengenai integritas dari informasi yang dikandungnya ketika muatan kontrak tersebut dibuat dalam bentuk akhir dalam bentuk suatu komunikasi elektronik; dan

b) bahwa kontrak secara elektronik memuat informasi yang dapat diakses (dibuka) kembali kepada orang yang hendak mengakses informasi yang terdapat dalam kontrak (yang dibuat secara elektronik) tersebut.

2.2.3. Tinjauan Umum Tentang Transaksi Elektronik

Berdasarkan ketentuan Pasal 1 butir (2) UU ITE, disebutkan bahwa transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer atau media elektronik lainnya. Transaksi jual beli secara elektronik merupakan salah satu perwujudan ketentuan di atas. Pada transaksi jual beli secara elektronik ini, para pihak yang terkait didalamnya, melakukan hubungan hukum yang dituangkan melalui suatu bentuk perjanjian atau kontrak yang juga dilakukan secara elektronik dan sesuai ketentuan Pasal 1 butir (17) UU ITE, disebut sebagai kontrak elektronik yakni perjanjian para pihak yang dibuat melalui Sistem Elektronik.

Pada transaksi jual beli secara elektronik, sama halnya dengan transaksi jual beli biasa yang dilakukan di dunia nyata, dilakukan oleh para pihak yang terkait, walaupun dalam jual beli secara elektronik ini pihak-pihaknya tidak bertemu secara

langsung satu sama lain, tetapi berhubungan melalui internet. Dalam transaksi jual beli secara elektronik, pihak-pihak yang terkait antara lain[68]:

a. Penjual atau *merchant* atau pengusaha yang menawarkan sebuah produk melalui internet sebagai pelaku usaha;
b. Pembeli atau konsumen yaitu setiap orang yang tidak dilarang oleh undang-undang, yang menerima penawaran dari penjual atau pelaku usaha dan berkeinginan untuk melakukan transaksi jual beli produk yang ditawarkan oleh penjual/pelaku usaha/*merchant*;
c. Bank sebagai pihak penyalur dana dari pembeli atau konsumen kepada penjual atau pelaku usaha/*merchant*, karena pada transaksi jual beli secara elektronik, penjual dan pembeli tidak berhadapan langsung, sebab mereka berada pada lokasi yang berbeda sehingga pembayaran dapat dilakukan melalui perantara dalam hal ini bank;
d. *Provider* sebagai penyedia jasa layanan akses internet.

Dikdik M. Arief Mansur dan Elisatris Gultom dalam bukunya "Cyberlaw"[69] mengutip Budhiyanto, yang mengidentifikasikan pihak-pihak yang terlibat terdiri dari:

a. Penjual (*merchant*), yaitu perusahaan/produsen yang menawarkan produknya melalui internet. Untuk menjadi *merchant*, maka seseorang/sebuah perusahaan harus mendaftarkan diri sebagai *merchant account* pada sebuah bank, tentunya ini dimaksudkan agar *merchant* dapat menerima pembayaran dari *customer* dalam bentuk *credit card*.
b. Konsumen / *card holder*, yaitu orang-orang yang ingin memperoleh produk (barang dan jasa) melalui pembelian secara *online*.
c. *Acquirer*, yaitu pihak perantara penagihan (antara penjual dan penerbit) dan perantara pembayaran (antara pemegang dan penerbit).
d. *Issuer*, perusahaan kartu kredit yang menerbitkan kartu kredit.

---

[68] Edmon Makarim, *Kompilasi Hukum Telematika*, (Jakarta :PT. RajaGrafindo Persada, 2000), hal.65.

[69] Lihat di Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyberlaw : Aspek Hukum Teknologi Informasi*, Cet Kesatu, (Bandung : PT Refika Aditama, 2005), hal. 152-153.

e. *Certification authority*, pihak ketiga yang netral yang memegang hak untuk mengeluarkan sertifikasi kepada *merchant*, kepada *issuer* dan dalam beberapa hal diberikan pula kepada *card holder*.

Transaksi jual beli secara elektronik merupakan hubungan hukum yang dilakukan dengan memadukan jaringan *(network)* dari sistem informasi yang berbasis komputer dengan sistem komunikasi yang berdasarkan jaringan dan jasa telekomunikasi.

Jenis-jenis Hubungan Hukum dalam *Electronic Commerce*

Hubungan hukum yang terjadi dalam transaksi jual beli secara elektronik tidak hanya tejadi antara pengusaha dengan konsumen saja, tetapi juga terjadi antara pihak-pihak dibawah ini[70]:

a. *Business to Business*, sering disebut sebagai *b to b*, merupakan transaksi yang terjadi antar perusahaan dalam hal ini, baik pembeli maupun penjual adalah sebuah perusahaan dan bukan perorangan. Biasanya transaksi ini dilakukan karena mereka telah saling mengetahui satu sama lain dan transaksi jual beli tersebut dilakukan untuk menjalin kerjasama antara perusahaan itu. Pertukaran informasi hanya berlangsung di antara mereka dan didasarkan pada kebutuhan dan kepercayaan.

b. *Business to Customer*, merupakan transaksi jual beli yang terjadi antara perusahaan dengan konsumen/individu. Contohnya adalah *amazon.com* sebuah situs *e-commerce* yang besar dan terkenal. Transaksi disebarkan secara umum dan konsumen yang berinisiatif melakukan transaksi. Produsen harus siap menerima respon dari konsumen tersebut. Biasanya sistem yang digunakan adalah sistem *web* karena sistem ini yang sudah umum dipakai oleh masyarakat.

c. *Customer to Customer*, merupakan transaksi jual beli yang terjadi antara individu dengan individu yang akan saling menjual barang.

---

[70] Lihat Edmon Makarim dan Deliana,*ibid.*, hal. 227-228.

d. *Customer to Business*, merupakan transaksi jual beli yang terjadi antara individu sebagai penjual dengan sebuah perusahaan sebagai pembelinya

e. *Customer to Government*, merupakan transaksi jual beli yang dilakukan antara individu dengan pemerintah, misalnya dalam pembayaran pajak.

Dengan demikian pihak-pihak yang dapat terlibat dalam suatu transaksi jual beli secara elektronik, tidak hanya antara individu dengan individu saja tetapi dapat individu dengan sebuah perusahaan, perusahaan dengan perusahaan atau bahka antara individu dengan pemerintah, dengan syarat bahwa para pihak termaksud secara perdata telah memenuhi persyaratan untuk dapat melakukan suatu perbuatan hukum dalam hal ini hubungan hukum jual beli.

Mekanisme Penawaran dan Penerimaan *Online*

Transaksi jual beli *e-commerce* juga merupakan suatu perjanjian jual beli sama dengan jual beli konvensional yang biasa dilakukan masyarakat. Hanya saja terletak perbedaan pada media yang digunakan. Pada transaksi *e-commerce*, yang dipergunakan adalah media elektronik yaitu internet. Sehingga kesepakatan ataupun perjanjian yang tercipta adalah melalui *online*.

Pada dasarnya proses transaksi jual beli secara elektronik tidak jauh berbeda dengan proses transaksi jual beli biasa di dunia nyata. Hampir sama dengan perjanjian jual beli pada umumnya, perjanjian jual beli *online* tersebut juga terdiri dari penawaran dan penerimaan. Sebab suatu kesepakatan selalu diawali dengan adanya penawaran oleh salah satu pihak dan penerimaan oleh pihak yang lain.

Pelaksanaan transaksi jual beli secara elektronik ini dilakukan dalam beberapa tahap, sebagai berikut [71]:

a. Penawaran, yang dilakukan oleh penjual atau pelaku usaha melalui *website* pada internet. Penjual atau pelaku usaha menyediakan *storefront* yang berisi katalog produk dan pelayanan yang akan diberikan. Masyarakat yang memasuki *website* pelaku usaha tersebut dapat melihat-lihat barang yang

[71] *Opcit.*, hal. 82.

ditawarkan oleh penjual. Salah satu keuntungan transaksi jual beli melalui di toko *on line* ini adalah bahwa pembeli dapat berbelanja kapan saja dan dimana saja tanpa dibatasi ruang dan waktu. Penawaran dalam sebuah *website* biasanya menampilkan barang-barang yang ditawarkan, harga, nilai rating atau *poll* otomatis tentang barang yang diisi oleh pembeli sebelumnya, spesifikasi barang termaksud dan menu produk lain yang berhubungan. Penawaran melalui internet terjadi apabila pihak lain yang menggunakan media internet memasuki situs milik penjual atau pelaku usaha yang melakukan penawaran, oleh karena itu, apabila seseorang tidak menggunakan media internet dan memasuki situs milik pelaku usaha yang menawarkan sebuah produk maka tidak dapat dikatakan ada penawaran. Dengan demikian penawaran melalui media internet hanya dapat terjadi apabila seseorang membuka situs yang menampilkan sebuah tawaran melalui internet tersebut.

b. Penerimaan, dapat dilakukan tergantung penawaran yang terjadi. Apabila penawaran dilakukan melalui *e-mail address*, maka penerimaan dilakukan melalui *e-mail*, karena penawaran hanya ditujukan pada sebuah *e-mail* yang dituju sehingga hanya pemegang *e-mail* tersebut yang dituju. Penawaran melalui *website* ditujukan untuk seluruh masyarakat yang membuka *website* tersebut, karena siapa saja dapat masuk ke dalam *website* yang berisikan penawaran atas suatu barang yang ditawarkan oleh penjual atau pelaku usaha. Setiap orang yang berminat untuk membeli barang yang ditawarkan itu dapat membuat kesepakatan dengan penjual atau pelaku usaha yang menawarkan barang tersebut. Pada transaksi jual beli secara elektronik, khususnya melalui *website*, biasanya calon pembeli akan memilih barang tertentu yang ditawarkan oleh penjual atau pelaku usaha, dan jika calon pembeli atau konsumen itu tertarik untuk membeli salah satu barang yang ditawarkan, maka barang itu akan disimpan terlebih dahulu sampai calon pembeli/konsumen merasa yakin akan pilihannya, selanjutnya pembeli/konsumen akan memasuki tahap pembayaran.

c. Pembayaran, dapat dilakukan baik secara langsung maupun tidak langsung, misalnya melalui fasilitas internet, namun tetap bertumpu pada sistem keuangan nasional, yang mengacu pada sistem keuangan lokal. Klasifikasi cara pembayaran dapat diklasifikasikan sebagai berikut [72]:

1) Transaksi model ATM, sebagai transaksi yang hanya melibatkan institusi finansial dan pemegang *account* yang akan melakukan pengambilan atau mendeposit uangnya dari *account* masing-masing;

2) Pembayaran dua pihak tanpa perantara, yang dapat dilakukan langsung antara kedua pihak tanpa perantara dengan menggunakan uang nasionalnya;

3) Pembayaran dengan perantaraan pihak ketiga, umumnya merupakan proses pembayaran yang menyangkut debet, kredit ataupun cek masuk. Metode pembayaran yang dapat digunakan antara lain : sistem pembayaran melalui kartu kredit *on line* serta sistem pembayaran *check in line*.

Apabila kedudukan penjual dengan pembeli berbeda, maka pembayaran dapat dilakukan melalui cara *account to account* atau pengalihan dari rekening pembeli kepada rekening penjual. Berdasarkan kemajuan teknologi, pembayaran dapat dilakukan melaui kartu kredit dengan cara memasukkan nomor kartu kredit pada formulir yang disediakan oleh penjual dalam penawarannya. Pembayaran dalam transaksi jual beli secara elektronik ini sulit untuk dilakukan secara langsung, karena adanya perbedaan lokasi antara penjual dengan pembeli, walaupun dimungkinkan untuk dilakukan.

d. Pengiriman, merupakan suatu proses yang dilakukan setelah pembayaran atas barang yang ditawarkan oleh penjual kepada pembeli, dalam hal ini pembeli berhak atas penerimaan barang termaksud. Pada kenyataannya, barang yang dijadikan objek perjanjian dikirimkan oleh penjual kepada pembeli dengan biaya pengiriman sebagaimana telah diperjanjikan antara penjual dan pembeli.

---

[72] *Ibid*, hal. 90.

Berdasarkan proses transaksi jual beli secara elektronik yang telah diuraikan diatas menggambarkan bahwa ternyata jual beli tidak hanya dapat dilakukan secara konvensional, dimana antara penjual dengan pembeli saling bertemu secara langsung, namun dapat juga hanya melalui media internet, sehingga orang yang saling berjauhan atau berada pada lokasi yang berbeda tetap dapat melakukan transaksi jual beli tanpa harus bersusah payah untuk saling bertemu secara langsung, sehingga meningkatkan efektifitas dan efisiensi waktu serta biaya baik bagi pihak penjual maupun pembeli.

Transaksi elektronik sebenarnya adalah transaksi yang terjadi karena adanya perikatan ataupun hubungan hukum yang dilakukan secara elektronik dengan memadukan jaringan (*networking*) dari sistem informasi berbasiskan komputer (*computer based information system*) dengan sistem komunikasi yang berdasarkan atas jaringan dan jasa telekomunikasi (*telecommunication based*), yang selanjutnya difasilitasi oleh keberadaan jaringan komputer global internet (*network of network*). Oleh karena itu, syarat sahnya perjanjian juga tergantung kepada esensi dari sistem elektronik itu sendiri. Sehingga, transaksi tersebut hanya dapat dikatakan sah bila dapat dijamin bahwa semua komponen dalam sistem elektronik itu dapat dipercaya dan/atau berjalan sebagaimana mestinya[73].

[73] Lihat Edmon Makarim dan Deliana,"Kajian Aspek Hukum Perikatan", dalam *Kompilasi Hukum Telematika* (Jakarta : PT RajaGrafindo Persada, 2003), hal. 223.

BAB 3

TRANSAKSI ELEKTRONIK YANG MELIBATKAN PENYELENGGARA SERTIFIKASI ELEKTRONIK (*CERTIFICATE AUTHORITY* ATAU CA)

3.1. KONSEP INFRASTRUKTUR KUNCI PUBLIK (*PUBLIC INFRASTRUCTURE KEY*)

3.1.1. Konsep Dasar Kriptografi

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[74]. 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*[75].

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

---

[74] 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. tersedia 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*

[75] 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*

a. *Confidentiality* (kerahasiaan); suatu pesan tidak boleh dapat dibaca atau diketahui oleh orang yang tidak berkepentingan.

b. *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.

c. *Integrity* (integritas/keutuhan); penerima harus merasa yakin bahwa pesan yang diterimanya tidak pernah diubah sejak pesan itu dikirim hingga diterima, seorang pengacau tidak dapat mengubah atau menukar isi pesan yang asli dengan yang palsu.

d. *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*)[76].

Dalam kriptografi, ada dua proses utama :

a. Enkripsi (*encryption*) : yakni proses untuk mengubah pesan asli (*plaintext*) menjadi pesan yang tersandikan atau pesan yang terahasiakan (*ciphertext*)

b. Dekripsi (*decryption*) : yakni proses mengubah pesan yang tersandikan (*ciphertext*) kembali menjadi pesan pada bentuk aslinya (*plaintext*).

Proses enkripsi dan dekripsi dengan menggunakan *key*[77]

Gambar 3.1.

[76] *Ibid.*

[77] Gambar proses enkripsi dan dekripsi tersedia di Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT-FHUI),*ibid.*, hal.18.

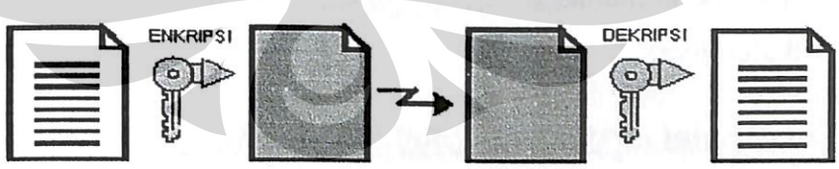
Kriptografi modern pada saat ini menggunakan "kunci" (*key*). Kunci ini menggantikan fungsi algoritma dalam proses *encryption*. Penggunaan kunci ini mempunyai berbagai kelebihan antara lain mudah didistribusikan secara meluas, sehingga banyak digunakan pada saat ini. Jadi meskipun penyerang (*hacker*) mengetahui secara tepat algoritma enkripsi dan dekripsinya, namun jika penyerang itu tidak memiliki kunci yang tepat , maka penyerang itu tidak bisa menjebol saluran komunikasi antara pengirim dan penerima.

Secara umum terdapat dua algoritma yang berbasis atau menggunakan kunci (*key-based algorithm*), yaitu *Symmetric* dan *Public-key*.

3.1.2. Kriptografi Kunci Simetrik

Ini adalah jenis kriptografi yang paling umum dipergunakan, sehingga seringkali disebut sebagai algoritma konvensional. Di dalam kebanyakan algoritma simetris kunci yang digunakan untuk melakukan *encryption* adalah sama dengan yang digunakan untuk melakukan *decryption*. Algortima ini sering juga disebut sebagai *secret-key algorithm, single-key algorithm, one-key algorithm* atau *symmetric key*[78].

Pesan yang akan dikirim akan di-*encrypt* terlebih dahulu sebelum dikirimkan. Setelah di-*encrypt ciphertext* tersebut barulah dikirimkan ke tujuannya. *Ciphertext* tersebut oleh penerima akan di-*decrypt* dengan menggunakan kunci yang sama yang digunakan untuk melakukan *encrypt*. Setelah proses *decrypt* inilah maka akan didapatkan kembali pesan yang asli.



Enkripsi Dan Dekripsi Pada Sebuah Dokumen

Gambar 3.2.

[78] Muhammad Aulia Adnan,*ibid.*,hal.25.

Contoh dari algoritma ini adalah DES (*Data Encryption Standard*). DES adalah algoritma yang dikembangkan oleh IBM dan dianggap sebagai algoritma yang aman. DES pada saat ini dalam penggunaannya telah dilipatgandakan keamanannya dengan *Triple DES.*

Meskipun algoritma ini mempunyai berbagai keunggulan dan kekuatan namun ia masih juga mempunyai kelemahan. Sistem kriptografi ini mempunyai beberapa kelemahan mendasar, yaitu :

a. Pengirim dan penerima menggunakan kunci yang sama, sehingga mereka masing-masing haruslah mempunyai kunci yang sama agar mereka dapat melakukan komunikasi. Mereka harus saling percaya bahwa tidak akan memberikan kunci tersebut kepada orang lain.

b. Pengirim dan penerima mempunyai kesulitan dalam mendistribusikan kunci tersebut. Pendistribusian kunci melalui jaringan internet adalah sangat berbahaya, karena siapa yang mempunyai kunci tersebut maka ia dapat membuka *ciphertext* yang dikirimkan. Problem ini bisa diatasi dengan mendistribusikan kunci melalui jalur komunikasi yang lain (*off band*).

Beberapa kelemahan seperti yang tersebut diatas menjadikan kelemahan teknik kriptografi ini bila digunakan di internet. Internet mengharuskan kita dapat berkomunikasi secara aman meskipun kita belum mengenal seseorang sebelumnya[79].

3.1.3. Kriptografi Kunci Publik / Kunci Asimetrik

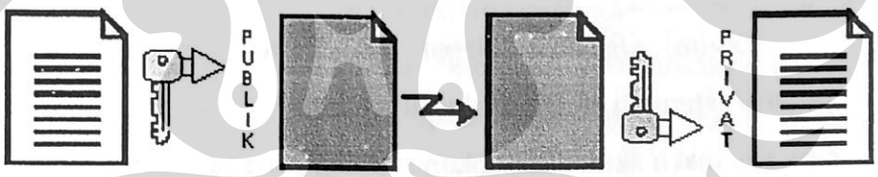
Teknik kriptografi kunci publik mencoba menjawab permasalahan pendistribusian kunci pada teknologi kriptografi kunci simetrik. *Public-key Algorithm* sering juga disebut sebagai algoritma asimetris adalah algoritma yang

[79] *Ibid.*, hal.26.

menggunakan kunci yang berbeda antara kunci yang digunakan untuk melakukan enkripsi dan yang digunakan untuk melakukan dekripsi. Dalam kriptografi kunci publik, setiap pihak memiliki sepasang kunci :

a. sebuah kunci publik (*public key*) yang didistribusikan kepada umum/ khalayak ramai.
b. sebuah kunci privat (*privat key*) yang harus disimpan dengan rahasia dan tidak boleh diketahui orang lain.

Algoritma ini dinamakan dengan algoritma kunci publik karena kunci yang akan digunakan untuk melakukan *encryption* (kunci publik) adalah dapat didistribusikan ke umum (publik). Seseorang yang tidak dikenal dapat saja menggunakan kunci tersebut untuk meng-*encrypt* suatu pesan, tetapi hanya orang tertentu saja (yaitu yang mempunyai kunci privat) yang dapat membuka pesan tersebut (mendenkrip). Kedua kunci tersebut (kunci privat dan kunci publik) mempunyai hubungan secara matematis, meskipun demikian seseorang yang mempunyai kunci publik tidaklah dapat membuat kunci privat dari kunci publik tersebut[80].



Enkripsi dan Dekripsi pada *Asymmetric Algorithm*

Gambar. 3.3.

Contoh dari algoritma ini adalah RSA (Rivest, Shamir, Adleman) dari RSA *Data Securities* dan DH (Diffie, Hellman), PGP (*Pretty Good Privacy*), *El-Gamal*, *Digital Signature Algorithm (DSA)* dan juga *Schnoor*[81].

---

[80] *Ibid.*

[81] *Ibid.*, hal.27.

3.1.4. Fungsi *Hash* Satu Arah

Fungsi *hash* satu arah atau *one-way hash function* mempunyai beberapa nama, seperti; *Compression Function, Message digest, Fingerprint, Message Integrity Check* (MIC). Fungsi utama dari fungsi *hash* ini adalah untuk memberikan suatu tanda yang unik yang berasal dari sebuah pesan yang hanya dipunyai oleh pesan tersebut. Fungsi ini adalah sesuai dengan penamaan fungsi ini seperti tersebut diatas yang dianalogikan sebagai sidik jari (*fingerprint*), atau pengecek keutuhan pesan (MIC)[82].

Fungsi *Hash*

Gambar 3.4.

3.1.5. Tanda Tangan Digital

Digital signature dapat dihasilkan baik dengan menggunakan algoritma simetris ataupun dengan algoritma kunci publik. Apabila menggunakan algoritma simetris maka akan dibutuhkan seorang perantara (*arbitrator*) dalam membuat sebuah *digital signature* yang aman. Pada saat ini *digital signature* biasanya dibuat dengan algoritma asimetris. Terdapat banyak algoritma kunci publik yang dapat digunakan untuk membuat *digital signature*. Salah satunya adalah RSA yang menggunakan kunci privat maupun kunci publik untuk melakukan enkripsi. Suatu dokumen akan dienkripsi dengan menggunakan sebuah kunci privat sehingga diperoleh suatu *digital signature* yang aman.

---

[82] *Ibid.*

Protokol dasar dari *digital signature* adalah:

a. Pengirim meng-*encrypt* dokumen dengan menggunakan kunci privat, sehingga ia menandatangani dokumen tersebut.
b. Ia kemudian mengirimkan dokumen tersebut ke penerima.
c. Penerima kemudian akan men-*decrypt* pesan tersebut dengan menggunakan kunci publik pengirim. Pada saat itulah ia akan melakukan verifikasi terhadap dokumen tersebut apakah benar dokumen tersebut berasal dari pengirim. Jika ia bisa membuka *ciphertext* tersebut maka ia dapat merasa yakin bahwa dokumen tersebut berasal dari pengirim[83].

Sifat yang diinginkan dari tanda tangan digital 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.

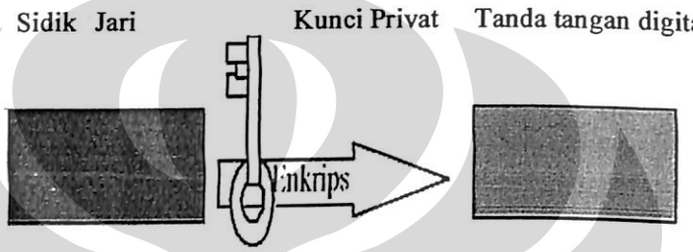
c. Tanda tangan itu dapat diperiksa dengan mudah.
d. Tanda tangan itu dapat diperiksa oleh pihak-pihak yang belum pernah bertemu dengan penandatangan.
e. Tanda tangan itu juga sah untuk kopi dari dokumen yang sama persis.

Meskipun ada banyak skenario, ada baiknya kita perhatikan salah satu skenario yang cukup umum dalam penggunaan tanda tangan digital. Tanda tangan digital

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

memanfaatkan fungsi hash satu arah untuk menjamin bahwa tanda tangan itu hanya berlaku untuk dokumen yang bersangkutan saja.

Bukan dokumen tersebut secara keseluruhan yang ditandatangani, namun biasanya yang ditandatangani adalah sidik jari dari dokumen itu beserta *time stamp*-nya dengan menggunakan kunci privat. *Time stamp* berguna untuk berguna untuk menentukan waktu pengesahan dokumen[84].



Pembuatan tanda tangan digital

Gambar 3.5.

Pada umumnya, tanda tangan digital menggunakan teknik kriptografi kunci publik, kunci simetrik dan sebuah fungsi hash satu arah. Patut dicatat bahwa tanda tangan digital bukanlah tanda tangan dari seseorang yang di-*scan* atau dimasukkan ke komputer menggunakan *stylus* atau *mouse,* tapi merupakan kumpulan dari kalkulasi-kalkulasi matematis untuk menyandikan data, yakni dengan kriptografi. Terminologi lain untuk *digital signature* adalah '*digitally ensured document*', agar maknanya tidak rancu. Jadi dapat diibaratkan sebagai dokumen yang sudah 'dikunci' dan tidak bisa dimanipulasi isinya[85].

---

[84] Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT-FHUI),*ibid.*, hal.22-23.

[85] Sri Wishnu Brata Prasetya dan FX Nursalim Hadi, "*Pengembangan Teknologi dan Aplikasi Teknologi Sekuriti Digital*", Riset Unggulan Terpadu Tahun 1998/1999, Fakultas Ilmu Komputer Universitas Indonesia dan **Kantor** Menteri Negara Riset

3.1.6. Tanda Tangan Elektronik

Menurut Pasal 1 butir (12) UU ITE maka yang dimaksud dengan tanda tangan elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentifikasi. Jadi tanda tangan elektronik adalah sistem pengamanan untuk melakukan transaksi elektronik yang digunakan sebagai alat verifikasi dan autentifikasi. Pengertian tanda tangan elektronik lebih luas dari pengertian tanda tangan digital.

3.1.7. Sertifikat Digital

Untuk mengamankan kunci publik, setiap kunci publik beserta keterangannya "disegel" dengan tanda tangan digital agar kunci publik dan keterangannya tidak bisa "dikutak-katik" oleh *hacker*. Ingat bahwa dengan menandatangani kunci publik dan keterangannya,berarti tidak ada yang bisa "memanipulasinya" lagi. Kalaupun ada yang mengubah-ubah,pasti akan ketahuan,karena tanda tangannya tidak akan *valid* lagi (lihat sifat tanda tangan digital).

Kunci publik beserta keterangan yang menyertainya yang sudah ditandatangani disebut dengan istilah sertifikat digital[86].

Keunggulan dari *public-key cryptography* dibandingkan dengan algoritma yang lain ternyata masih menyimpan kelemahan dalam hal keamanan (*security*), kelemahan ini adalah adanya kemungkinan pihak ke-3 yang tidak berhak menukar kunci publik milik seseorang dengan kunci miliknya. Juga terdapat ketidakpastian tentang identitas dari pemilik kunci publik. Kelemahan ini akan mengurangi keamanan dari sistem *public-key crypthography* karena seseorang dapat dengan mudah mengatakan bahwa suatu dokumen yang telah ditandatanganinya adalah tidak sah karena kuncinya telah diambil atau mengatakan bahwa kunci itu adalah bukan

---

Dan Teknologi Dewan Riset Nasional, tersedia di *http://www.geocities.com/amwibowo/resource/rut6/laporan.html*

[86] *Ibid.*, hal.24.

miliknya. Untuk mengatasi hal ini dibutuhkan adanya pihak ke-3 yang terpercaya (*Trusted Third Party*/TTP) yang dinamakan otoritas sertifikat (*Certification Authority*/CA/OS[87]) yang akan menghubungkan kunci dengan pemiliknya. Ia akan menerbitkan suatu sertifikat yang berisi identitas dari seseorang dan juga kunci privat dari orang tersebut.

Secara umum tugas dari *Certification Authority* adalah sebagai berikut:

a. Membuat kunci publik/privat miliknya sendiri.
b. Melakukan verifikasi terhadap identitas seorang calon pelanggan yang hendak meminta sertifikat dari *certification authority* tersebut. Verifikasi ini adalah berdasarkan patokan atau standar yang sudah ditentukan sebelumnya.
c. Pelanggan kemudian menyerahkan kunci publiknya kepada *certification authority*.
d. *Certification authority* kemudian mencek apakah kunci tersebut adalah pasangan dari kunci privat yang dipunyai calon pelanggan tersebut.
e. Apabila semua persyaratan tersebut sudah dipenuhi maka *certification authority* akan menerbitkan sebuah sertifikat digital (*digital certificate*) atas nama orang tersebut. *Digital certificate* tersebut berisi kunci duplikat dari kunci publik pelanggan dan juga identitas dari pelanggan. *Certification Authority* kemudian akan menandatangani *digital certificate* tersebut dengan menggunakan kunci privat miliknya[88].

3.1.7. Transaksi Elektronik Dengan Kriptografi

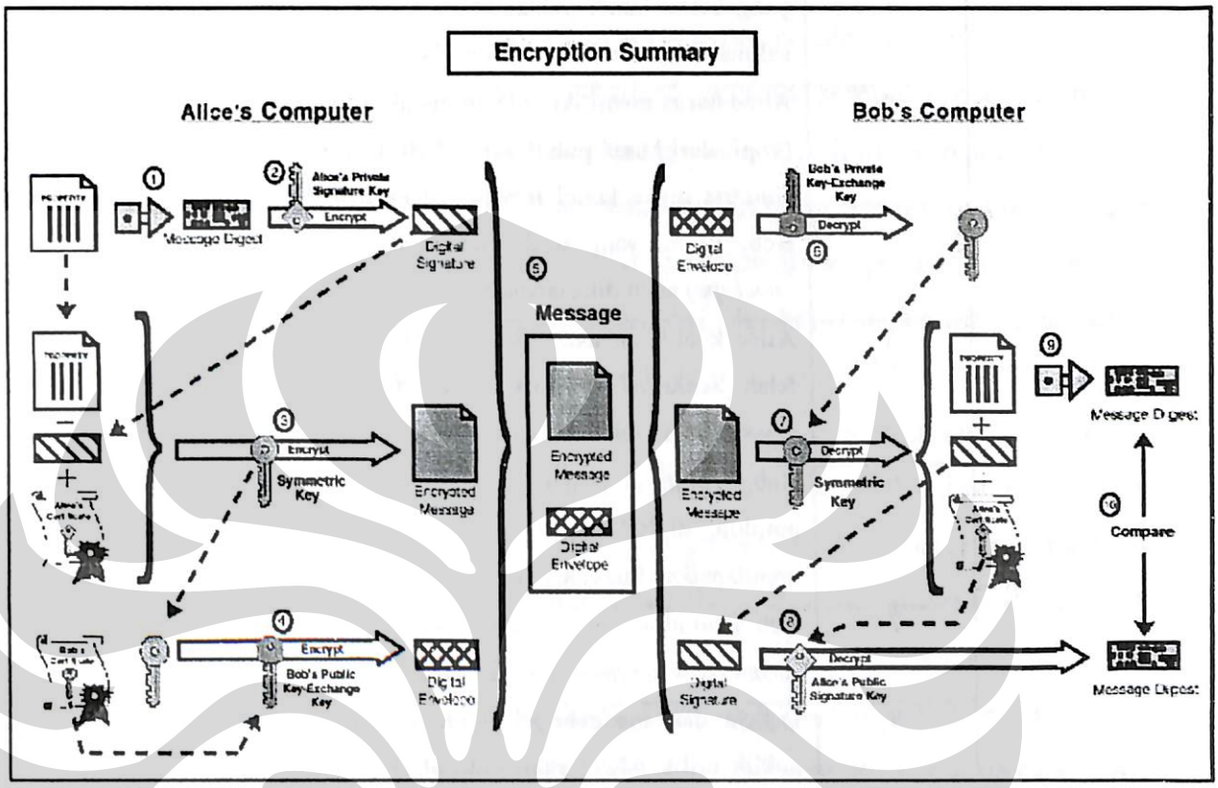
Penggunaan kriptografi atau *public-key algorithm* dalam menandatangani suatu dokumen akan menimbulkan kerumitan-kerumitan. Dibawah ini akan diterangkan dalam bentuk ringkasan (*summary*) tentang proses tandatangan digital.

---

[87] Working Group on Electronic Commerce of Japan, *Certification Authority Guidelines version 1.0* (Tokyo:ECOM,1998), hal.1.

[88] Muhammad Aulia Adnan, *ibid.*, hal.30-31.

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



Rangkuman Dari Penggunaan Kriptografi

Gambar 3.6.

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 teradap *message digest* tersebut dengan menggunakan kunci privatnya sehingga ia akan mendapatkan digital signature dari data tersebut.

3	Kemudian, Alice membuat (*generates*) suatu kunci simetris secara acak (*random*) dan 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 bersamasama 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[89]

Gambar 3.7.

[89] Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT-FHUI),*ibid.*, hal.27-28.

3.2. *CERTIFICATE AUTHORITY* (CA) SEBAGAI *TRUSTED THIRD PARTY* DALAM TRANSAKSI ELEKTRONIK

Transaksi *e-commerce* sebagaimana telah diterangkan sebelumnya, melibatkan beberapa pihak, baik yang terlibat secara langsung maupun tidak lansung, tergantung kompleksitas transaksi yang dilakukan. Artinya apakah semua proses transaksi dilakukan secara *online* atau hanya beberapa tahap saja yang dilakukan secara *online*. Apabila transaksi *e-commerce* tidak sepenuhnya dilakukan secara online, dengan kata lain hanya proses transaksinya saja yang online, sementara pembayarannya tetap dilakukan secara manual melalui tunai/cash atau transfer bank, maka pihak *acquirer, issuer* dan *certification authority* (CA) tidak terlibat di dalamnya[90].

Untuk menjalankan *e-commerce*, dibutuhkan tingkat keamanan yang dapat diterima. *E-commerce* yang menggunakan *internet* relatif bersifat tidak aman, *open* dan memanfaatkan *open system*. Di dunia internet relatif sulit sekali memastikan apakah seseorang itu benar *personal* yang dimaksud sehingga timbul permasalahan mendasar dalam pemanfaatan *e-commerce*.

Dalam komunikasi *online* harus memenuhi lima persyaratan hukum, yang sebenarnya juga merupakan persyaratan hukum dalam mekanisme non-elektronik. Meskipun tidak seluruh persyaratan dapat diterapkan dalam segala situasi, namun biasanya terdiri dari[91]:

a. *Authenticity* (otentisitas)

Persyaratan ini berkaitan dengan otentisitas/keaslian pihak yang terlibat dalam suatu komunikasi online. Dari mana suatu pesan berasal, apakah pesan tersebut berasal dari orang yang berwenang? Persyaratan ini merupakan persyaratan praktek dalam bisnis pada umumnya termasuk dalam praktek notaris. Dalam perdagangan tradisional hal tersebut dilakukan dengan surat yang ditanda-tangani.

---

[90] Dikdik, *opcit.*, hal.154.

[91] Lihat Thomas J. Smendinghoff, ed., *Online Law: The SPA's Legal Guide To Doing Business On The Internet* (USA: Addison Wesley Developers Press, 1996), hal. 24-32.

Dalam Kitab Undang-Undang Hukum Perdata disyaratkan untuk beberapa hal perlu dibuat akta otentik, misalnya surat wasiat, akta hibah, akta pemindahan hak dan pembebanan hak atas kebendaan tak bergerak. Suatu akta dikatakan otentik apabila mempunyai bentuk yang telah ditentukan undang-undang dan dan dibuat oleh atau dihadapan pegawai umum yang berwenang untuk itu ditempat dimana akta itu dibuat[92]. Pejabat yang berwenang membuat akta otentik sebagaimana dimaksud dalam KUH Perdata adalah notaris[93]. Akta itu merupakan alat bukti yang berkekuatan pembuktian sempurna[94]. *Authenticity* juga merupakan persyaratan hukum di dunia virtual atau Internet, karena menyangkut masalah pertanggungjawaban. Dalam *authenticity* terkandung pula suatu kewenangan seseorang untuk melakukan sesuatu. Seorang kandidat notaris atau notaris yang belum diambil sumpahnya membuat suatu akta, maka akta itu tidak dapat dikatakan otentik, karena si pembuat akta tidak berwenang, sekalipun cakap sebagai notaris. Demikian pula dalam komunikasi *online* di Internet akan memenuhi syarat *authenticity* apabila orang yang melakukan komunikasi *online* itu adalah benar-benar orang yang cakap dan berwenang untuk melakukannya. Semua pihak harus benar-benar memperhatikan syarat ini atau jika tidak maka akan terjadi suatu perselisihan. Untuk itu diperlukan suatu hal-hal pendukung yang dapat memastikan persyaratan ini dipenuhi, yaitu: *Digital Signature*, *Certificate Authority* (CA) dan mungkin nantinya diperlukan *electronic notary* (*e-notary/cyber notary*).

b. *Integrity* (keutuhan)

Persyaratan ini berkaitan dengan ketepatan dan kelengkapan suatu komunikasi. Pesan, data atau informasi yang dikirim dan yang diterima haruslah sama dan lengkap. Pesan, data atau informasi itu bukan pesan hasil rekayasa ataupun pesan,

---

[92] Kitab Undang-Undang Hukum Perdata [Burgelijke Wetboek], *op. cit.*, Psl.1868.

[93] Diatur di Pasal 1 butir (1) Undang-Undang No. 30 Tahun 2004 Tentang Jabatan Notaris, disahkan dan diundangkan di Jakarta serta mulai berlaku pada tanggal 6 Oktober 2004 (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 117, Tambahan Lembaran Negara Republik Indonesia Nomor 4432)

[94] Kitab Undang-Undang Hukum Perdata, *op. cit.*, Psl.1871.

data atau informasi yang tidak utuh. Dalam mekanisme non-elektronik, *integrity* dapat ditemukan pada penggunaan tinta permanen yang tidak dapat dihapus. Dalam praktek notaris persyaratan *integrity* dapat ditemukan dalam bentuk akta yang sudah tertentu, yaitu kepala akta, komparisi, premise, isi akta dan akhir akta. Ketidaklengkapan bagian akta menyebabkan syarat *integrity* ini tidak dipenuhi. Apabila syarat ini tidak dipenuhi, maka informasi, komunikasi dan dokumen elektronik yang disampaikan tidaklah sah dan tidak memberikan kepastian hukum sehingga dapat menimbulkan perselisihan antara pihak yang terlibat didalamnya. Untuk menunjang terpenuhinya persyaratan ini diperlukan infrastruktur penunjang seperti: *public key infrastructure*.

c. *Nonrepudiation*

Para pihak yang berkomunikasi tidak dapat menyangkal mengenai apa yang telah dilakukan dalam komunikasi *online* tersebut. Persyaratan ini sangat mendasar bagi transaksi elektronik dimana para pihak mengandalkan komunikasi secara elektronik. Dalam praktek notaris syarat ini dapat ditemukan pada komparisi yang didukung dengan bukti-bukti pendukung identitas seperti: Kartu Tanda Penduduk, kutipan akta kelahiran yang fotokopinya dilekatkan pada minuta akta dan pemenuhan syarat ini ditemukan juga pada akhir akta dimana notaris membacakan isi akta kepada para penghadap dan para saksi untuk kemudian para pihak yang menghadap, para saksi dan notaris sendiri menandatangani akta yang dibuat. Dengan demikian akta tersebut tidak dapat disangkal pembuatannya, keberadaannya dan kebenarannya oleh para pihak yang menghadap.

d. *Writing and signature*

Dalam banyak kasus terdapat persyaratan adanya bukti tertulis (hitam atas putih) dan tanda tangan para pihak yang terlibat. Hal ini tentu penting guna pembuktian apabila terjadi suatu perselisihan. Persyaratan ini bertalian erat dengan persyaratan *nonrepudiation* tersebut di atas dan untuk menjamin terpenuhinya persyaratan ini diperlukan adanya infrastruktur *digital signature*.

e. *Confidentiality/Privacy*

Pengendalian informasi yang diketahui para pihak. Dalam perdagangan tradisional surat ditulis dalam amplop dan lalu ditanda-tangani lalu di-*seal*. Persyaratan ini sangat penting untuk melindungi kerahasiaan seseorang, sebagai contoh: nomor kartu kredit, rekam medis seseorang, data atau informasi rahasia dan penting milik perusahaan, minuta akta. Data penting yang dikomunikasikan secara *online* penting untuk dilindungi, jika tidak mungkin ada orang-orang yang menyalahgunakannya untuk kepentingan sendiri. Untuk melindungi kerahasiaan data elektronik digunakan teknik enkripsi dengan berbagai metode antara lain *public key infrastruktur (PKI)* dan *pretty good privacy (PDP)*.

Salah satu cara untuk meningkatkan keamanan dalam *e-commerce* adalah dengan menggunakan teknologi *kriptografi*, yaitu antara lain dengan menggunakan *enkripsi* untuk mengacak data. Salah satu metoda yang mulai umum digunakan adalah pengamanan informasi dengan menggunakan *public key system*. Sistem lain yang bisa digunakan adalah *private key system*. Infrastruktur yang dibentuk oleh sistem public key ini disebut *Public Key Infrastructure* (PKI), atau diterjemahkan dalam Bahasa Indonesia menjadi Infrastruktur Kunci Publik (IKP), dimana kunci publik dapat dikelola untuk pengguna yang tersebar (di seluruh dunia). Salah satu komponen dari infrastruktur kunci publik[95] ini adalah *certification authority* (CA) yang merupakan sebuah *body / entity* yang memberikan dan mengelola sertifikat

---

[95] Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT-FHUI),*ibid.*, hal.30.

Menurut RFC 2510 tentang manajemen sertifikat , dalam sebuah model *public key infrastructure* terdapat beberapa entitas :

1. *Subject* atau *subscriber* : yakni orang-orang yang *memiliki* sertifikat digital dengan dirinya (namanya) tertera sebagai " *subject*" dalam sertifikat digital tersebut.
2. *Certification Authority* (CA) : entitas yang namanya tertera sebagai "issuer" pada sebuah sertifikat digital
3. *Registration Authority* (RA) : pihak yang dipercaya oleh CA untuk melakukan proses otentikasi dan verifikasi terhadap jati diri *subsriber/subject*. Penandatanganan tetap dilakukan oleh CA.
4. *Certificate Repository* : yakni suatu tempat untuk mendistribusikan sertifikat yang sudah disahkan oleh CA , maupun tempat untuk mendistribusikan daftar sertifikat yang dibatalkan (*Certificate Revocation List / CRL*)
5. *Relying Party* : orang yang melakukan transaksi bisnis dengan mempercayai sertifikat digital dari orang lain (biasanya mitra transaksinya)

digital yang dibutuhkan dalam transaksi elektronik. CA berhubungan erat dengan pengelolaan *public key system*[96]. Contoh sebuah CA di Amerika adalah Verisign[97].

Certification/Certificate Authority (CA) baik berupa perorangan maupun badan hukum yang berfungsi sebagai pihak ketiga (*Trusted third party*) yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik/digital serta menyediakan layanan keamanan yang dapat dipercaya oleh pengguna dalam menjalankan pertukaran informasi secara elektronis dan memenuhi empat aspek keamanan (*Confidentiality; Authentification; Integrity; Non repudiation*)[98].

Certification Authority (CA) memastikan atau menegaskan identitas seseorang (*subscriber),* dan bertugas menyatakan bahwa kunci publik dari pasangan kunci publik-privat yang digunakan untuk membuat *digital signature*[99] adalah milik orang tersebut. CA akan mengeluarkan suatu sertifikat berbasis komputer (sertifikat digital

---

[96] Lihat Budi Rahardjo, *Mengimplementasikan Electronic Commerce di Indonesia, 31* Juli 1999, tersedia di http://www.cert.or.id/~budi/articles/1999-02.pdf

[97] VeriSign, sebuah otoritas sertifikat publik yang didirikan pada bulan Mei 1995, menyediakan sertifikat digital untuk produk-produk terkenal dari Netscape dan Microsoft. Visa juga telah memilih VeriSign sebagai otoritas sertifikat yang dipergunakannya dalam implementasi protokol *Secure Electronic Transaction* (SET) yang dirancang oleh Visa dan MasterCard. Namun pihak MasterCard dan American Express memilih GTE CyberTrust sebagai otoritas sertifikat yang dipercaya. GTE memang memiliki pengalaman 10 tahun dalam membuat sertifikat digital untuk pemerintah federal Amerika Serikat. Berbeda dengan GTE, VeriSign lebih mengkonsentrasikan dirinya pada pemberian sertifikat digital untuk individu atau badan usaha umum. Tersedia di Arrianto Mukti Wibowo, *Tanda tangan digital & sertifikat digital: Apa itu?*, artikel ini muncul pada Infokomputer edisi Internet Juni 1998, tersedia di http://www.geocities.com/amwibowo/resource/sertifik/tanya.html

[98] Ahmad M.Ramli, Gunung, Pager., Apriadi, Indra., *Menuju Kepastian Hukum di Bidang Informasi dan Transaksi Elektronik*, (Jakarta : Depkominfo RI, Agustus 2006).

[99] Dalam Lampiran Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2006 tentang Pedoman Penyelenggaraan *Certification Authority* (CA) di Indonesia yang dimaksud dengan Tanda Tangan Digital adalah tanda tangan yang dihasilkan dengan menandatangani *Message Digest* yang bersifat *unique* untuk setiap *message,* menggunakan kunci pribadi pengguna.

Bandingkan dengan definisi dalam Pasal 1 butir (12) UU ITE bahwa Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

atau SD)[100] yang menyatakan hubungan antara suatu kunci publik dan *subcriber* yang diidentifikasi. Dalam sertifikat tersebut terdapat kunci publik *subscriber* dan informasi lain yang diperlukan seperti tanggal masa berlakunya kunci publik. Untuk menjamin keaslian dan keutuhan isi sertifikat tersebut, CA membubuhkan *digital signature* CA pada sertifikat.

Proses sertifikasi untuk mendapatkan pengesahan dari C.A. dapat dibagi menjadi tiga tahap :

a. Pelanggan/*subscriber* membuat sendiri pasangan kunci privat dan kunci publiknya dengan menggunakan *software* yang ada di dalam komputernya
b. Menunjukan bukti-bukti identitas dirinya seperti: Surat Izin Mengemudi (SIM), paspor atau bukti identitas sesuai dengan yang disyaratkan C.A.
c. Membuktikan bahwa dia mempunyai kunci privat yang dapat dipasangkan dengan kunci publik tanpa harus memperlihatkan kunci privatnya.

Tahapan-tahapan tersebut tidak mutlak harus seperti di atas, akan tetapi tergantung pada ketentuan-ketentuan yang telah ditetapkan oleh C.A. itu sendiri. Hal ini berkaitan dengan level/tingkatan dari sertifikat yang diterbitkannya dan level/tingkatan ini berkaitan juga dengan besarnya kewenangan yang diperoleh

---

[100] Lihat M Iqbal Suparta, *Sistem Keamanan Perdagangan Elektronik Dengan Teknologi Secure Electronic Transaction (SET)*, TUGAS MATA KULIAH EC-7010 (KEAMANAN SISTEM LANJUT) di www.cert.or.id/~budi/courses/ec7010/dikmenjur/iqbal-report-2.pdf
Dalam sebuah transaksi jual beli yang dilakukan melalui internet di mana kedua belah pihak tidak saling bertemu, harus ada suatu mekanisme tertentu yang menjamin identitas kedua pihak tersebut. Tidak ada pihak yang mau ditipu, bertransaksi dengan orang yang menyamar jadi orang lain atau dengan orang yang tidak memiliki sesuatu yang dapat ditransaksikan, namun hanya berpura-pura.
Sertifikat digital adalah informasi mengenai identitas pemilik sertifikat yang ditandatangani secara digital oleh sebuah badan independen yang menjamin bahwa si pemilik sertifikat layak untuk ikut dalam transaksi jual beli tersebut. Badan independent ini disebut *Certificate Authority* (CA). Termasuk dalam informasi yang terdapat dalam sertifikat digital adalah kunci publik, sehingga sertifikat digital ini juga merupakan mekanisme pertukaran kunci publik. Sertifikat digital ini selain mempunyai hubungan dengan kunci publik dan identitas pemilik, ia juga memiliki hubungan yang sangat erat dengan nomor rekening bank pemilik sertifikat ini. Walaupun tidak secara langsung informasi rekening bank ini tercantum dalam sertifikat, CA menyimpan nomor rekening tersebut dalam basis data miliknya, sehinggga nomor rekening tersebut dapat diasosiasikan dengan sertifikatnya.

pelanggan/*subscriber* berdasarkan sertifikat yang didapatkannya. Semakin besar kewenangannya yang diperoleh dari suatu *Digital Certificate* yang diterbitkan oleh C.A. semakin tinggi pula level sertifikat yang diperoleh serta semakin ketat pula persyaratan yang ditetapkan oleh C.A. Sebagai contoh; untuk mendapatkan suatu sertifikat yang mempunyai level kewenangan yang cukup tinggi, terkadang C.A. bahkan memerlukan kehadiran secara fisik si *subscriber* sehingga C.A. dapat memperoleh kepastian pihak yang akan memperoleh sertifikat tersebut.

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

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

a. Identitas C.A. yang menerbitkannya.
b. Pemegang/pemilik/*subscriber* dari sertifikat tersebut.
c. Batas waktu keberlakuan sertifikat tersebut.
d. Kunci publik dari pemilik sertifikat.

Setelah sertifikat tersebut diumumkan maka pihak-pihak lain dapat melakukan transaksi, transfer pesan dan berbagai kegiatan dengan media internet secara aman dengan pihak pemilik sertifikat.

Fungsi-fungsi C.A. yang telah kita bicarakan di atas dapat kita golongkan sebagai berikut :

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

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

a. Penjual (*merchant*)
b. Pembeli (*buyer*)
c. *Certification/Certificate Authority* (CA)

Selanjutnya, ada juga para pihak yang andilnya tidak kalah penting, yaitu :

d. *Account Issuer* (penerbit rekening contoh: kartu kredit)
e. Jaringan pembayaran (contohnya Visa dan Mastercard dalam *scheme* SET)
f. Internet *Service Provider* (ISP)
g. Internet *Backbones*[101]

Perusahaan atau lembaga C.A yang biasa digunakan di internet antara lain, VeriSign, Thawte, GeoTrust, Comodo, CaCert.org[102].

Sertifikat dipublikasikan dengan cara direkam dalam satu atau lebih *repository*/penyimpanan atau disebarkan dengan cara lainnya dengan tujuan agar sertifikat itu dapat diakses oleh setiap orang yang hendak berkomunikasi dengan *subscriber*. *Repository* hampir sama dengan *yellow pages digital* dimana merupakan

---

[101] Tinjauan Kritis Atas CA (Certificate/ *Certification Authority*) RUU ITE dalam Presfektif Akademis
Tersedia di *http://209.85.175.104/search?q=cache:leWIbdXXpc4J:www.mti.ugm.ac.id/~slamet/kuliah/Aspek_Legal/uu/tugas%2520pak%2520ongkokel%25205/Tugas%2520Aspek%2520Legal%2520-%2520Tinjauan%2520kritis%2520RUU%2520ITE%2520CA.doc+pengaturan+certification+authority+di+amerika&hl=id&ct=clnk&cd=4&gl=id*

[102] Anonim, *Certificate Authority* , www.wikipedia.org, 2007.

basis data sertifikat-sertifikat yang dapat diakses *online* dan dapat diakses oleh siapapun. *Repository* ini dikelola oleh CA. Guna melindungi para pihak dalam transaksi, maka diperlukan *Certification Practice Statements*[103], *Certificate Revocation Lists, Certification Expiration, Limits Liability.*

Sertifikat digital diterbitkan oleh otoritas sertifikat (OS) atau CA. Seseorang atau suatu badan mendapatkan sertifikat digital jika sudah mendaftarkan diri mereka kepada otoritas sertifikat atau CA. CA atau otoritas sertikat tidak hanya menerbitkan sertifikat saja, namun juga memeriksa apakah suatu sertifikat digital masih berlaku atau tidak. Otoritas sertifikat selain memiliki daftar sertifikat digital yang telah diterbitkannya, juga memiliki apa yang disebut dengan daftar sertifikat yang dibatalkan (*certificate revocation list*). Daftar sertifikat terbatalkan (DSB) itu berisi sertifikat-sertifikat apa saja yang sudah tidak berlaku lagi karena tercuri, hilang atau ada perubahan identitas (misalnya perubahan alamat surat elektronik dan alamat rumah). Setiap kali ada pihak yang ingin memeriksa sertifikat digital, ia dapat menghubungi otoritas sertifikat secara *on-line* untuk memastikan bahwa sertifikat yang diterimanya masih berlaku. Jika semakin banyak sertifikat yang dibatalkan, tentu otoritas sertifikat akan terbebani dan akan memperlambat proses pemeriksaan sertifikat digital yang ingin diuji keabsahannya. Oleh karena itu, dalam sertifikat digital terdapat tanggal kadaluarsa. Sertifikat digital yang sudah melampaui tanggal kadaluarsa akan dihapus dari dalam DSB, karena tidak ada pihak manapun yang akan mau memeriksa sertifikat digital yang sudah kadaluarsa[104].

---

[103] *Certification Practice Statement* merupakan pernyataan tertulis yang menjelaskan secara detil bagaimana CA yang bersangkutan menjalankan prakteknya (registrasi, penerbitan, pencabutan, dan lain-lain). CPS bisa juga berupa kontrak antara CA *subscriber*. Atau merupakan dokumen komposit yang terdiri dari hukum publik, kontrak CA subscriber atau deklarasi dari CA. Hal penting dalam CPS ini adalah: hak dan kewajiban dari para pihak, tanggungjawab kemungkinan kerugian, masalah keamanan CA, biaya, masalah audit, masalah kerahasiaan serta interpretasi akan *statement* (pernyataan) tersebut. Dapat dibaca selengkapnya di *http://209.85.175.104/search?q=cache:s3GTydeEwbEJ:onno.vlsm.org/v01/OnnoWPurbo/contrib/aplikasi/hukum/lokakarya-regulasi-e-commerce-dalam-era-digital-ekonomi-05-20.rtf+pengaturan+certification+authority+di+amerika&hl=id&ct=clnk&cd=2&gl=id*

[104] Arrianto Mukti Wibowo, *ibid.*

Berbicara tentang CA, terdapat hirarki kedudukan di antara mereka. Sebuah CA dapat memiliki sertifikat yang ditandatangani oleh CA di tingkat atasnya, demikian pula CA di tingkat atasnya tersebut dapat memiliki sertifikat yang ditandatangani oleh CA di tingkat lebih atasnya lagi, begitu seterusnya sampai *Root CA*. Sertifikat milik *Root CA*[105] ditandatangani oleh dirinya sendiri. Karena tingkatan sertifikat itu identik dengan tingkatan kunci publik, maka *Root CA* sering disebut *Root Key*.

Pada sistem perdagangan di internet yang menggunakan sertifikat digital, bagian rentan adalah keabsahan sertifikat milik otoritas sertifikat utama yang didistribusikan kepada konsumen. Oleh karena itu umumnya sertifikat digital milik Otoritas Sertifikat utama (yang berisi kunci publik OS utama) dijadikan bagian yang integral dalam program aplikasi. Kalau diperhatikan lebih jeli lagi, sebenarnya yang penting adalah bagaimana pihak pengembang perangkat lunak bisa mendapatkan sertifikat digital milik OS utama yang terjamin keasliannya.

VeriSign, sebuah otoritas sertifikat publik yang didirikan pada bulan Mei 1995, menyediakan sertifikat digital untuk produk-produk terkenal dari Netscape dan Microsoft. Visa juga telah memilih VeriSign sebagai otoritas sertifikat yang dipergunakannya dalam implementasi protokol *Secure Electronic Transaction* (SET) yang dirancang oleh Visa dan MasterCard. Namun pihak MasterCard dan American Express memilih GTE CyberTrust sebagai otoritas sertifikat yang dipercaya. GTE memang memiliki pengalaman 10 tahun dalam membuat sertifikat digital untuk pemerintah federal Amerika Serikat. Berbeda dengan GTE, VeriSign lebih

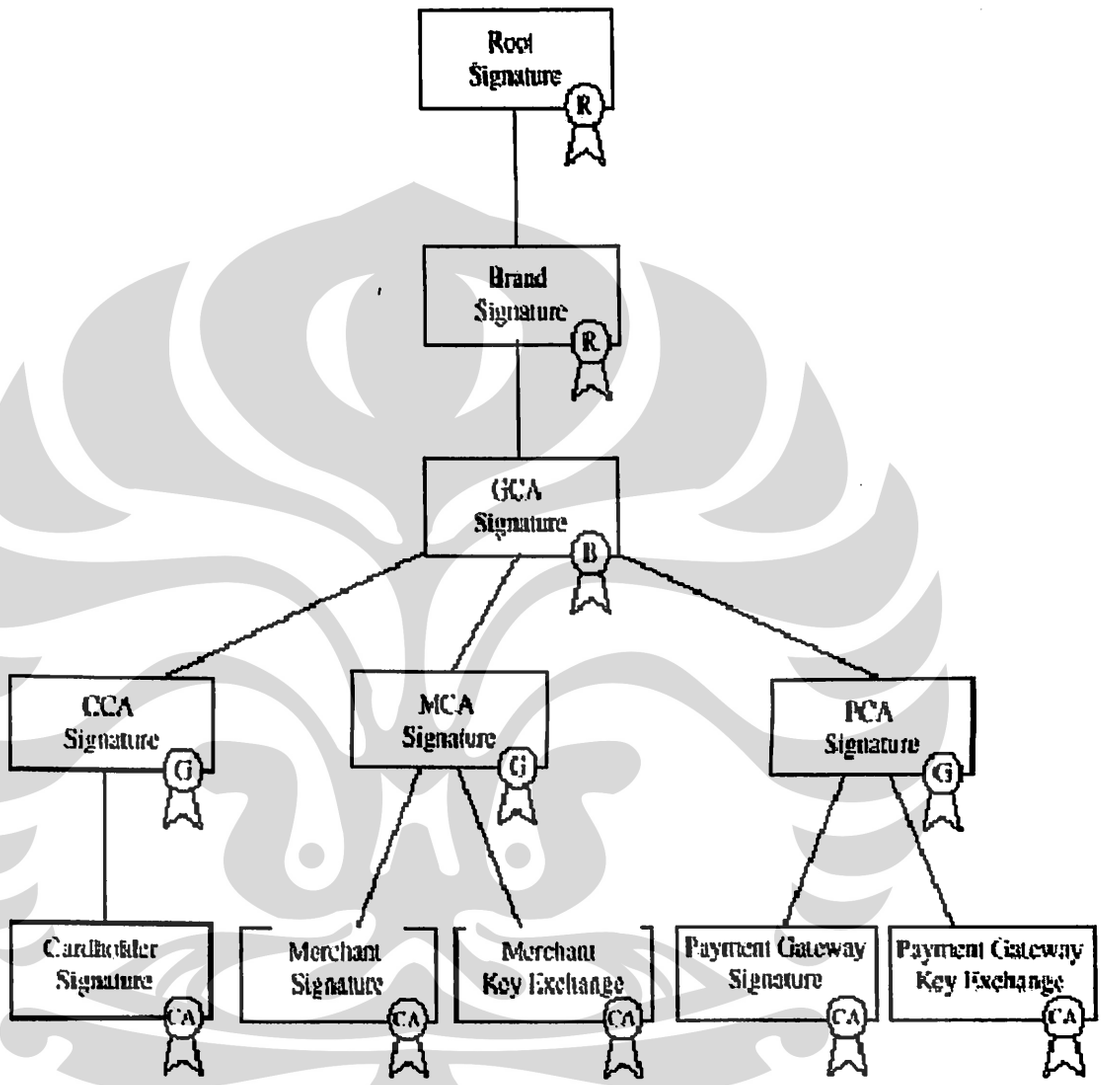
---

[105] Dalam Lampiran Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2006 tentang Pedoman Penyelenggaraan *Certification Authority* (CA) di Indonesia yang dimaksud dengan *Root CA* adalah sebuah lembaga/unit yang berfungsi menandatangani kunci publik *{digital certificate)* CA, mengatur dan menjalankan proses *cross CA*.

Bandingkan menurut Arrianto Mukti Wibowo, *Tanda tangan digital & sertifikat digital: Apa itu?*, Artikel, (Jakarta :Infokomputer edisi Internet, Juni 1998), tersedia di *http://www.geocities.com/amwibowo/resource/sertifik/tanya.html*

Otoritas sertifikat publik yang memberikan izin kepada pihak lain untuk menjadi otoritas sertifikat sering disebut otoritas sertifikat utama (*root certificate authority*).

mengkonsentrasikan dirinya pada pemberian sertifikat digital untuk individu atau badan usaha umum[106].



Hirarki Kepercayaan *Certificate Authority* (CA)

Gambar 3.8.

[106] Arrianto Mukti Wibowo,*ibid.*

Pada gambar dapat kita lihat terdapat bermacam-macam CA. Terdapat *Cardholder* CA (CCA) yang mengeluarkan sertifikat *cardholder*, *Merchant* CA (MCA) yang mengeluarkan sertifikat *merchant*, *Payment Gateway* CA (PCA) yang mengeluarkan sertifikat *payment gateway*, *Geopolitical* CA (GCA) yang menaungi CA-CA dalam satu negara, *Brand* yang menaungi CA-CA dalam satu merek tertentu, dan yang paling atas adalah *Root*. Masing-masing sertifikat CA tersebut memiliki hubungan ke sertifikat CA di tingkat atasnya, terutama melalui tanda tangan CA di tingkat atasnya.

Saat ini kita mungkin memiliki pertanyaan bahwa *carholder*, *merchant*, dan *payment gateway* juga perlu jaminan ketika sedang berhubungan dengan sebuah CA. *Certificate Authority* (CA) tentu memiliki sertifikat, namun bagaimana cara memverifikasi sertifikat CA tersebut. Ada beberapa fakta singkat yang menggambarkan hal itu, yakni:

Seluruh vendor yang menyediakan perangkat lunak bagi *cardholder*, *merchant*, maupun *payment gateway* telah mempunyai hubungan dengan suatu Root CA. Mereka menyisipkan sertifikat *root* dalam setiap perangkat lunak yang mereka pasarkan. *Cardholder*, *merchant* dan *payment gateway* ketika melakukan registrasi sertifikat pada suatu CA; selain diberikan kembali sertifikat milik mereka sendiri, juga diberikan kumpulan sertifikat para CA. *Cardholder*, *merchant* dan *payment gateway* menelusuri jalur tanda-tangan sertifikat-sertifikat CA tersebut mulai dari sertifikat CA yang akan diverifikasi sampai ke sertifikat *root*. Kemudian sertifikat *root* yang ada dalam kumpulan sertifikat tersebut dibandingkan dengan sertifikat *root* yang tersimpan dalam perangkat lunak keluaran *vendor* dan harus sama.

BAB 4

PENGATURAN IZIN OPERASI / LISENSI PENYELENGGARA SERTIFIKASI ELEKTRONIK (*CERTIFICATE AUTHORITY* ATAU C.A.) ASING

4.1. TINJAUAN UMUM TENTANG IZIN OPERASI / LISENSI *CERTIFICATE AUTHORITY*

4.1.1. Pentingnya izin operasi / lisensi C.A.

Tujuan perizinan operasi CA adalah meningkatkan kepercayaan pelanggan terhadap SD yang dikeluarkan CA dan untuk memberikan kepastian hukum. Izin operasi bagi CA ditetapkan atau dicabut oleh Menteri Komunikasi dan Informatika berdasarkan pertimbangan dan usulan BP-CA[107].

4.1.2. Pentingnya pendaftaran C.A.

a. Untuk memberikan kepastian hukum yaitu domisili tergugat yang jelas

CA asing yang tidak terdaftar atau terdaftar di Indonesia artinya tidak mempunyai domisili di Indonesia maka jika CA asing tersebut dalam operasionalnya mengakibatkan kerugian pada pengguna SDnya maka si pengguna SD tersebut hanya dapat menggugat CA asing yang tidak terdaftar tersebut di negara asal dimana CA tersebut didirikan sehingga tidak ada perlindungan hukum menurut hukum Indonesia. Lain halnya jika CA asing itu pun mendirikan kantor perwakilan atau badan hukum di Indonesia, seperti yang diatur dalam *Digital Signature Act (DSA)* 1997 Malaysia, maka berdasarkan hukum acara perdata bahwa gugatan terhadap suatu badan hukum diajukan ke Pengadilan Negeri yang daerah hukumnya meliputi

[107] Lampiran Permeninfo No.29 Tahun 2006, hal.30-31.

tempat kedudukan dari badan hukum yang disebutkan dalam anggaran dasarnya[108]. Hal tersebut diatur dalam Pasal 118 ayat (1) HIR[109] dan Pasal 142 ayat (1) RBg[110]. Jika CA asing mendirikan kantor perwakilan atau badan hukum di Indonesia, artinya pengguna SD mendapatkan perlindungan hukum lebih pasti dengan dapat menggugat CA asing di Indonesia.

b. Melindungi kepentingan masyarakat dari risiko kerugian akibat perbuatan CA yang tidak bertanggungjawab

Jadi pendaftaran CA itu penting untuk menjamin kepastian hukum dan menjaga fungsi kepercayaan dari CA dimaksud[111]. Untuk menjamin interoperabilitas dalam berbagai aplikasi bisnis, kunci kriptografis yang diterbitkan agar memenuhi standar yang mengatur persyaratan kemampuan CA yaitu SNI 19-7125-2005, Teknologi Informasi - Teknik Keamanan - Panduan Teknik untuk Penggunaan dan Manajemen Jasa Pihak Ketiga Terpercaya. Sedangkan pengamanan infrastruktur CA persyaratan yang dipenuhi CA adalah ISO/IEC 17799 : 2005, *Information Technology -Security Techniques - Code of Practices For Information Security Management* (Teknologi Informasi – Kode Pengaturan Manajemen Pengamanan Informasi) dan ISO/IE C 27001 : 2005, *Information Technology - Security Technique - Certification Criteria for Information Security Management System - Requirement*[112].

---

[108] http://library.usu.ac.id/download/fh/perdata-muhammad.pdf

[109] http://www.legalitas.org/database/staatsblad/stb44-1941.pdf

Pasal 118.

(1) Tuntutan (gugatan) perdata yang pada tingkat pertama termasuk lingkup wewenang pengadilan negeri, harus diajukan dengan surat permintaan (surat gugatan) yang ditandatangan oleh penggugat, atau oleh wakilnya menurut pasal 123, kepada ketua pengadilan negeri di tempat diam si tergugat, atau jika tempat diamnya tidak diketahui, kepada ketua pengadilan negeri di tempat tinggalnya yang sebenamya. (KUHPerd. 15; IR. 101 .)

[110] http://www.legalitas.org/database/staatsblad/stb227-1927.pdf

Pasal 142

(1) Gugatan-gugatan perdata dalam tingkat pertama yang menjadi wewenang pengadilan negeri dilakukan oleh penggugat atau oleh seorang kuasanya yang diangkat menurut ketentuan-ketentuan tersebut dalam pasal 147, dengan suatu surat permohonan yang ditanda-tangani olehnya atau oleh kuasa tersebut dan disampaikan kepada ketua pengadilan negeri yang menguasai wilayah hukum tempat tinggal tergugat atau, jika tempat tinggalnya tidak diketahui di tempat tinggalnya yang sebenarnya.

[111] Lihat maksud dan tujuan dari Permeninfo No. 29 Tahun 2006, hal.3.

[112] *Ibid.*,hal.20-21.

Maka diatur kriteria CA antara lain :

1) Terdaftar (*registered*) dalam transaksi *e-commerce*

Keabsahan bahwa CA yang bersangkutan memiliki kompetensi dan kredibilitas teknis namun tidak menjamin legalitas bisnis CA yang dilakukannya (resiko ditanggung sendiri).

2) Berlisensi (*licenced*) dalam transaksi *e-commerce*

Keabsahan bahwa CA yang bersangkutan memiliki kompetensi dan kredibilitas teknis (sertifikasi oleh LS-CA) dan keabsahan bahwa CA yang bersangkutan memiliki landasan *legal* berbisnis CA sektor Privat (lisensi oleh BP-CA).

3) Terakreditasi (*accredited*) dalam *e-government* dan lain-lain

Keabsahan bahwa CA yang bersangkutan memiliki kompetensi dan kredibilitas teknis (sertifikasi oleh LS-CA), memiliki landasan legal berbisnis CA sektor publik (lisensi oleh BP-CA) serta terakreditasi untuk berbisnis CA instansi Pemerintah

c. *Cross border certificate*

SD yang diterbitkan oleh CA yang terdaftar dan terakreditasi di Indonesia dapat diakui eksistensinya dalam transaksi elektronik yang lintas batas Negara/ *cross border*[113] atau di luar wilayah Indonesia.

4.1.3. Dampak ijin operasi/lisensi dan akreditasi terhadap status tandatangan elektronik

Kepemilikan izin operasi dari CA membawa akibat hukum terhadap status tandatangan elektronik yaitu bagi CA yang tidak terdaftar di Indonesia misalnya CA-CA untuk penggunaan secara terbatas di lingkungan sendiri misalnya untuk absen di kantor atau tanda pengenal mahasiswa di kampus maka tidak diperlukan pendaftaran CA sedangkan status tandatangan elektronik dari pengguna SD di lingkungan terbatas tersebut hanya berlaku untuk di wilayah tersebut. Untuk perdagangan elektronik maka ada dua skema CA yaitu terdaftar dan terakreditasi, cukup jelas bahwa kedudukan CA yang terakreditasi lebih kuat/*creditable* daripada CA yang

[113] Ibid., hal. 11. Dimana hukum nasional, Indonesia, mengatur CA sebagai subyek hukum di Indonesia dan mengakui eksistensi keberadaan CA internasional yang eksis sesuai hukum domisili CA tersebut

terdaftar maka status tandatangan elektronik dari CA yang terakreditasi juga lebih *accredited* daripada tandatangan elektronik dari CA yang terdaftar.

4.2. STATUS PERJANJIAN ELEKTRONIK YANG MENGGUNAKAN PENYELENGGARA SERTIFIKASI ELEKTRONIK (*CERTIFICATE AUTHORITY* ATAU C.A.) ASING

Permasalahan yang timbul mengenai legalitas perjanjian elektronik difokuskan menjadi tiga isu kunci, yaitu masalah keabsahan (*validity*), pelaksanaan (*enforceability*), dan pengakuan (*admisibility*) dari metode-metode elektronik yang dilakukan dalam perdagangan[114].

4.2.1. Keabsahan (*validity*) perjanjian elektronik yang menggunakan penyelenggara sertifikasi elektronik (*certificate authority* atau C.A.) asing[115]

Perjanjian apapun bentuknya, *online* atau tidak, dapat berbentuk lisan maupun tertulis. Semuanya dimulai dengan adanya kesepakatan (*a meeting of mind*) antara para pihak, serta berlaku dan mengikat bagi para pihak layaknya undang-undang (*pacta sunt servanda*) bagi yang membuatnya.

Asas penting mengenai lahirnya perjanjian adalah asas konsensualisme yaitu suatu kontrak dianggap lahir dan mengikat ketika tercapai kata sepakat[116] dan berlaku universal.

Mengenai kesepakatan sebagaimana diatur dalam Pasal 20 UU ITE :

---

[114]Ian Walden, *Computer Crime and Digital Investigations*, (New Yorks, Oxford University Press Inc, 2007) hal. 354- 355.

[115] Lihat Rosa Agustina, "Undang-Undang Informasi Dan Transaksi Elektronik Dan Hukum Perikatan Internasional", paper dalam Diskusi Ahli dengan Tema "Dinamika Terkini Konvergensi Hukum Telematika Dalam Sistem Hukum Nasional Indonesia", Hotel Ina Kuta,Bali, 12 Juli 2008.

[116]Subekti, Hukum Perjanjian, (Jakarta: PT. Intermasa, 2002), hal. 15. Lihat juga William R. Anson, *Principles of the English Law of Contract*, (Oxford: AG Guest University Press, 1961) hal. 4. mengatakan bahwa pertemuan keinginan dari para pihak dalam sebuah perjanjian yang penuh dan finak; maka haruslah ada konsensus.

(1) Kecuali ditentukan lain oleh para pihak, Transaksi Elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima.

(2) Persetujuan atas penawaran Transaksi Elektronik sebagaimana dimaksud pada ayat (1) harus dilakukan dengan pernyataan penerimaan secara elektronik.

Teori mengenai kesepakatan sebagaimana termaksud dalam Pasal 20 UU ITE selain tidak ditentukan lain adalah teori Penerimaan (*acceptance theory*).

Dalam menganalisis kontrak-kontrak yang lahir dengan perantaraan teknologi informasi *incasu* internet ada dua teori utama terkait dengan teori lahirnya kesepakatan, yaitu (1) teori penerimaan (*acceptance theory*) dan (2) teori kotak surat (*mailbox theory*). Penggunaannya didasarkan dari metode pengkomunikasian dari informasi tersebut apakah bersifat seketika (*instantaneous*) atau tidak (*no instantaneous*). Apabila waktu pengkomunikasiannya seketika maka teori yang diterapkan adalah teori penerimaan, sedangkan untuk waktu pengkomunikasian yang tidak seketika maka digunakan teori kotak surat (*mailbox theory*).

Secara umum, kontrak elektronik dengan media atau alat internet (baca: kontrak *online*) dapat dilakukan dengan dua cara, email dan world wide web (www)[117]. Permasalahannya kemudian muncul kapan terjadinya kesepakatan antara para pihak yang melakukan perjanjian tersebut. Kesepakatan dalam kontrak online via e-mail terjadi sebagian besar berkisar antara kapan tawaran diterima oleh pihak yang berhak menerima informasi (baca: penerima) sampai kapan penerima membaca dan atau mengkonfirmasi kembali. Sementara kontrak elektronik *via website* (www) kesulitannya terjadi dalam menentukan apakah kesepakatan terjadi dengan satu klik, dua klik, atau tiga klik[118].

Keabsahan atau kevaliditasan sebuah kontrak elektronik dalam hukum perjanjian baik dalam sistem hukum *common law* maupun *civil law* adalah

---

[117]Assafa Endeshaw, *Internet dan E-commerce Law with a Focus on Asia Pasific*, (Singapore: Prentice Hall, 2001), hal. 245.

[118]Setiawan, "Electronic Commerce: Tinjauan dari Segi Kontrak," (makalah disampaikan pada seminar Legal Aspects of E-Commerce, Jakarta, Agustus 2000), hal. 4. yang dikutip oleh Edmon Makarim, Kompilasi Hukum Telematika, (Jakarta: PT. Raja Grafindo Persada, 2003), hal. 235.

bergantung pada terpenuhinya syarat-syarat perjanjian. Sehingga dapat dikatakan bahwa apabila syarat-syarat tersebut terpenuhi, perjanjian atau kontrak tersebut dapat dinyatakan sah. Berdasarkan hukum Indonesia, mengenai syarat sahnya perjanjian diatur dalam Pasal 1320 KUH Perdata, dimana syarat-syarat tersebut adalah : pertama, sepakat bagi mereka yang mengikatkan dirinya, kedua, cakap untuk membuat perjanjian, ketiga, suatu hal tertentu, dan keempat, suatu sebab (kausa) yang halal.

Keabsahan atau kevaliditasan sebuah kontrak elektronik yang menggunakan penyelenggara sertifikasi elektronik (*certificate authority* atau C.A.) asing yang terdaftar atau tidak terdaftar tidak mempengaruhi status keabsahan kontrak elektronik itu sendiri, karena sepanjang memenuhi syarat-syarat pembentukan kontrak atau syarat sahnya suatu perjanjian maka perjanjian elektronik tersebut sah demi hukum, kecuali apabila tidak memenuhi syarat subyektif maka perjanjian tersebut dapat dimintakan pembatalan sedangkan jika tidak terpenuhi sayarat obyektif maka perjanjian elektronik tersebut batal demi hukum. Di mana mengenai syarat subyektif tentang kecakapan para pihak dapat dilihat dari Sertfikat Digital yang menjelaskan identitas para pihak apakah orang yang berwenang membuat perjanjian tersebut atau orang yang bersangkutan sesuai dengan isi SDnya, dimana SD dikeluarkan oleh CA.

4.2.2 Pelaksanaan *(enforceability)* perjanjian elektronik yang menggunakan penyelenggara sertifikasi elektronik *(certificate authority* atau C.A.) asing

Pelaksanaan kontrak disini adalah bagaimana kontrak itu dilaksanakan. Dalam pelaksanaan ini ada dua isu yang ditemukan yaitu: pertama, isu mengenai pembayaran dan kedua bagaimana menjamin pelaksanaan tersebut dengan kriptografi dan tanda tangan elektronik (*digital signatures*).

Pelaksanaan yang penting dari seorang pembeli adalah melakukan pembayaran, apabila ada kontrak jual beli. Salah satu cara melakukan pembayaran secara *online* yang paling umum adalah dengan menggunakan kartu kredit. Setidaknya ada tiga cara pembayaran dengan menggunakan kartu kredit, yaitu:

a. Pembeli mengirimkan informasi mengenai kartu kreditnya melalui email.

b. Informasi kartu kredit adalah disandikan misalkan dengan menggunakan teknologi *Secure Sockets Layer* untuk mengamankan selama transaksi online tersebut berlangsung.

c. Cara yang ketiga adalah melibatkan sistem enkripsi kunci privat, artinya antara penjual dan pembeli menyandarkan pada dua kombinasi kunci privat dan publik untuk melindungi transaksi yang dilakukan[119].

Cara untuk menjamin pelaksanaan tersebut dengan kriptografi dan tanda tangan elektronik (*digital signatures*) yaitu dengan menggunakan jasa dari penyelenggara sertifikasi elektronik (*certificate authority* atau C.A.).

4.2.3. Pengakuan *(admisibility)* perjanjian elektronik yang menggunakan penyelenggara sertifikasi elektronik (*certificate authority* atau C.A.) asing

Transaksi yang dilakukan secara elektronik sudah barang tentu menghasilkan informasi elektronik yang tertuang pada media digital (elektronik). Hal ini berbeda dengan transaksi yang dilakukan dengan berbasiskan kertas maka informasi tercetak di media kertas. Sehingga pengakuan terhadap informasi atau dokumen elektronik yang dihasilkan oleh transaksi elektronik itu menjadi perlu. Terutama jika dihadapkan dengan hal pembuktian.

Atas dasar itulah UU ITE juga memberikan pengakuan terhadap informasi dan/atau dokumen elektronik khususnya dalam hal pembuktian. Sebagaimana tertuang dalam Pasal 5 UU ITE.

(1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

(2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

---

[119] Murtha, Cullina, Richter and Pinney, "The Internet and the Chancing Internet Landscape", *http://www.mcrp.com/ip9-99.pdf*

4.3. PERBANDINGAN PENGATURAN IZIN OPERASI / LISENSI PENYELENGGARA SERTIFIKASI ELEKTRONIK (*CERTIFICATE AUTHORITY* ATAU CA) ASING DI INDONESIA DENGAN DI NEGARA LAINNYA MISALNYA UNI EROPA, INGGRIS, AMERIKA SERIKAT, NEGARA BAGIAN WASHINGTON, SINGAPURA DAN MALAYSIA

Untuk melihat pengaturan mengenai ijin operasi/lisensi penyelenggara sertifikasi elektronik (*certificate authority* atau CA) maka Penulis akan menjelaskan tentang pengaturan ijin operasi / lisensi penyelenggara sertifikasi elektronik (*certificate authority* atau CA) asing di Indonesia dan di Negara lainnya misalnya di Uni Eropa dalam *Directive* 1999/93/EC pada 13 Desember 1999 tentang Tanda Tangan Elektronik, Inggris dengan *Electronic Communications Act* 2000 dan *the Electronic Signatures Regulations* 2002 (*the Regulations*), Amerika Serikat dengan *Uniform Electronic Transactions Act* (UETA), Negara Bagian Washington dengan *Electronic Authentication Act*, serta Negara Asia yang terdekat denagn Negara kita yaitu Singapura dengan *Electronic Transactions Act* dan Malaysia dengan *Digital Signature Act*, baru setelah itu di Indonesia dengan UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Peraturan Menteri Komunikasi dan Informatika. Setelah itu akan dijabarkan pembahasan usulan untuk rancangan Peraturan Menteri Komunikasi dan Informatika tentang CA yang baru sehubungan dengan telah diundangkannya UU ITE.

Penyelenggara Sertifikasi Elektronik atau *Certification Authority* (CA) di Indonesia diatur dalam peraturan Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, secara teknis dalam Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2006 tentang Pedoman Penyelenggaraan *Certification Authority* (CA) di Indonesia dan Peraturan Menteri Komunikasi dan Informatika No. 30 Tahun 2006 tentang Badan Pengawas *Certification Authority*.

Pasal 1 butir (10) UU ITE mengatur definisi

> "Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik".

Definisi ini memperjelas tujuan utama yang diperankan oleh "penyelenggara sertifikasi elektronis" yaitu menerbitkan sertifikat elektronik atas tanda tangan elektronik, karena identitas dan status subyek hukum Penandatangan dipastikan ketika diterbitkannya sertifikat elektronik.

Selain tujuan utama ini, penyelenggara sertifikasi elektronis dapat menyediakan pelayanan-pelayanan lainnya yang bertujuan untuk menunjang penyelenggaraan tanda tangan elektronik agar mampu mengikuti evolusi teknologi, misalnya dengan menyediakan jasa *time stamping*[120], jasa pembuatan kunci publik, pengarsipan elektronis36 dan lain-lainnya. Sehingga, menurut penulis, lebih tepat Pasal 1 butir (10) ini didefinisikan sebagai berikut, "subyek hukum yang berfungsi sebagai pihak ketiga yang layak dipercaya, yang yang memberikan dan mengaudit Sertifikat Elektronik serta menyediakan pelayanan-pelayanan yang berkaitan dengan penyelenggaraan tanda tangan elektronik".

Dalam Pasal 13 UU ITE diatur bahwa Penyelenggara Sertifikasi Elektronik terdiri atas Penyelenggara Sertifikasi Elektronik Indonesia dan Penyelenggara Sertifikasi Elektronik asing[121], dimana Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia[122] serta Penyelenggara Sertifikasi Elektronik asing yang beroperasi di Indonesia harus terdaftar di Indonesia[123]. Ketentuan mengenai Penyelenggara Sertifikasi Elektronik asing akan diatur lebih lanjut dengan Peraturan Pemerintah[124]. Menurut salah satu penguji[125], Dr. Inosentius Samsul, SH MH, melihat pentingnya peranan dari

---

[120] Sebuah teknik untuk membubuhkan keterangan waktu pada dokumen elektronik. Teknik ini merupakan salah satu teknik untuk mengetahui waktu terjadinya kesepakatan dalam kontrak. Dokumen-dokumen yang telah ditandatangani secara elektronis dikirim ke *server* utama dari *horodatage* (dalam bahasa inggris, *time stamp server*). *Server* ini sendiri yang akan memberikan keterangan waktu yang tepat pada dokumen-dokumen tersebut. Dapat dibaca selengkapnya di Julius I.D. Singara, *La cryptologie et la Preuve Electronique de la France àl'Indonésie,* thesis dari D.E.A. Informatique et Droit, Université Montpellier I, Tahun akademik 2003-2004, hal.80. atau di Julius Indra Dwipayono Singara, *Pengakuan Tanda Tangan Elektronik Dalam Hukum Pembuktian Indonesia*, di catatan kaki ke-35 di hal. 11. *http://www.legalitas.org/database/artikel/pidana/esign.pdf*

[121] Pasal 13 ayat (3) UU ITE

[122] Pasal 13 ayat (4) UU ITE

[123] Pasal 13 ayat (5) UU ITE

[124] Pasal 13 ayat (6) UU ITE

[125] Ujian tesis tanggal 25 Juli 2008 pukul 14.00-15.00 WIB di Ruang F, Pascasarjana Salemba, Jakarta

penyelenggara sertifikasi elektronik sebagai pihak yang menyediakan sistem sekuriti untuk menjamin keamanan bertransaksi secara elektronik, maka sebaiknya aturan hukum mengenai CA diatur dalam Undang-Undang, bukan dalam Peraturan Pemerintah.

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

1) metode yang digunakan untuk mengidentifikasi PenandaTangan;
2) hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda Tangan Elektronik; dan
3) hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik[126].

Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2006 tentang Pedoman Penyelenggaraan *Certification Authority* (CA) di Indonesia[127] lahir dilatarbelakangi oleh diperlukannya pengamanan dalam rangka pertukaran informasi melalui internet yang terkait dengan transaksi bisnis atau perdagangan secara elektronik. Pedoman Penyelenggaraan CA di Indonesia diperlukan untuk dapat dijadikan dasar pengorganisasian CA, pengawasan penyelenggaraan CA, pengamanan penggunaan CA pada transaksi elektronik, pengamanan infrastruktur CA dan peran pemerintah untuk memberikan kepastian hukum dan melindungi kepentingan masyarakat dari risiko kerugian akibat perbuatan CA yang tidak bertanggung jawab. Dalam Permeninfo ini juga diatur Lembaga Sertifikasi CA (LS-CA) diberi kewenangan untuk melakukan Penilaian Kesesuaian CA terhadap Standar Nasional Indonesia (SNI) yang dipersyaratkan.

Secara umum bentuk organisasi CA harus memiliki elemen-elemen antara lain[128] :

a) Berbentuk badan hukum Indonesia dan beroperasi di Indonesia, serta memiliki izin operasi CA dari Menteri Komunikasi dan Informatika berdasarkan

---

[126] Pasal 14 UU ITE

[127] Peraturan ini mulai berlaku pada tanggal ditetapkan di Jakarta pada tanggal 2 Nopember 2006.

[128] Lihat di Lampiran Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2006 tentang Pedoman Penyelenggaraan *Certification Authority* (CA) di Indonesia, hal. 11-13.

pertimbangan dan usulan dari BP-CA;

b) Memiliki peran *cross border,* berarti hukum nasional mengatur keberadaan CA yang ada sebagai subyek hukum di Indonesia dan hukum nasional mengakui eksistensi keberadaan CA internasional yang eksis sesuai hukum tempat domisili CA tersebut;

c) Sebagai subyek hukum, CA sebagai pihak ketiga terpercaya yang memberikan kepastian/pengesahan identitas pelanggan dan pengesahan pasangan kunci publik dan kunci pribadi;

d) Layanan CA terbuka dan dapat diakses oleh seluruh aplikan (pemohon) yang membutuhkan CA;

e) Independen dan tidak memihak;

f) Memiliki fungsi manajemen dalam sistem operasinya sesuai kriteria sertifikasi SNI yang dipersyaratkan dan memenuhi persyaratan/kesesuaian standar manajemen (ISO/IEC 27001: 2005, *Information Technology - Security Technique Information Security Management System Requirement),* yaitu :

   (1) *Policy Authority* yang bertanggung jawab menetapkan kebijakan tertulis *Certificate Policy* (CP) dan *Certification Practice Statement* (CPS), serta melakukan *management review* untuk mengevaluasi dan melakukan perbaikan terhadap pelaksanaan CPS;

   (2) *Registration Authority* yang bertanggung jawab memverifikasi data identitas pemegang sertifikat dan memvalidasi kebenarannya;

   (3) *Certificate Issuer* bertanggung jawab menerbitkan kunci kriptografi atau memvalidasi kunci kriptografi apabila kunci tersebut diterbitkan oleh pihak lain, serta melaksanakan pembuatan, pembubuhan tanda tangan CA dan publikasi serta pemeliharaan SD;

   (4) *Repository Service* yang bertanggung jawab mempublikasikan CP, CPS, SD dan *revocation status bulletin,* baik melalui *repository* yang dimiliki oleh CA maupun oleh pihak lain;

(5) *Revocation Management* yang bertanggung jawab mengawasi penyalahgunaan SD, menyelidiki kebenaran pengaduan yang diterima, menentukan langkah langkah yang harus dilakukan sehubungan dengan pembekuan atau pembatalan SD, serta menyusun *revocation status bulletin,*

g) Status personal badan hukum CA tunduk sepenuhnya kepada hukum Indonesia;

h) Personal CA harus orang yang kompeten, memenuhi kualifikasi dan terlatih, bersertifikat/lisensi untuk kriteria teknis tertentu, menguasai teknis SNI terkait, komunikatif lisan dan tertulis, bebas dari konflik kepentingan.

Fungsi CA adalah[129]:

a) Memfasilitasi transaksi elektronik antara pihak Pertama dan Kedua melalui penerbitan SD yang berisi kunci publik dan konfirmasi terhadap identitas pemegang kunci publik atau pelanggan;

b) Memberikan otentifikasi terhadap kunci publik para pihak yang melakukan transaksi elektronik;

c) Memastikan identitas dan status subyek hukum penanda-tangan selama masa berlakunya tanda tangan digital. Tanda tangan digital ini memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:

(1) Data pembuatan tanda tangan terkait hanya kepada penanda tangan saja (pemilik kunci pribadi);

(2) Data pembuatan tanda tangan digital pada saat proses penandatanganan hanya berada dalam kuasa penandatangan;

(3) Segala perubahan terhadap tanda tangan digital yang terjadi setelah waktu penandatanganan dapat diketahui;

(4) Segala perubahan terhadap informasi elektronik yang terkait dengan tanda tangan digital tersebut setelah waktu penandatanganan dapat diketahui;

---

[129] *Ibid.*, hal.13-15.

(5) Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatangannya;

(6) Terdapat cara tertentu untuk menunjukkan bahwa penandatangan telah memberikan persetujuan terhadap informasi elekronik yang terkait dengan tanda tangan digital;

d) Melakukan verifikasi, pemeriksaan dan pembuktian identitas pengguna dan pelanggan serta mensahkan pasangan kunci publik dengan identitas pemiliknya;

e) Administratif mencakup registrasi, otentifikasi fisik, pembuatan dan pengelolaan kunci, pengelolaan dan pembekuan SD;

f) Menyediakan directory tentang status dari SD yang diterbitkannya;

g) Dapat dilengkapi dengan tembaga pelaksana registrasi yang menjalankan fungsi administratif;

h) Dapat mendelegasikan fungsi registrasi dan publikasi kepada sebuah Otoritas Registrasi atau Penyedia Jasa *Repository* (tempat untuk menyimpan dan mengumumkan SD yang siap diakses oleh publik), namun tanggung jawab tetap berada pada CA.

Kewajiban Legal CA adalah[130] :

a) Memberitahukan segala keterangan yang berkaitan dengan penawaran dan permintaan yang diajukan oleh para pihak dalam transaksi elektronik;

b) Menjaga kerahasiaan identitas pengguna jasa dan pelanggan dari pihak yang tidak berkepentingan;

c) Bertanggung jawab penuh terhadap SD yang diterbitkan;

d) Mengenal dan menguasai bidang transaksi bisnis/ perdagangan yang dilayani, lingkup layanan dan batas tanggung jawab yang dituangkan dalam kebijakan tertulis (CP);

e) Membuat dan memelihara dokumentasi arsip secara sistematik dan dapat dipertanggungjawabkan dalam bentuk *paper based, e-Based* dan bentuk lain yang

[130] *Ibid.*, hal.15-16.

diperbolehkan;

f) Membuat laporan kepada BP-CA berkaitan dengan aspek perusahaan, aktivitas terkait dengan perizinan, keuangan, SD dan kendala/hambatan yang dihadapi;

g) Mempublikasikan SD yang dibekukan atau dicabut, setelah menerima permintaan pembekuan atau pencabutan SD.

h) Mengizinkan Lembaga Pengawasan yaitu LS-CA untuk melakukan audit tanpa harus membahayakan faktor-faktor keamanan operasional CA, baik diminta atau atas laporan pihak ketiga.

Persyaratan Legal CA adalah[131] :

a) Berbadan hukum Indonesia dan beroperasi di Indonesia;

b) Memperoleh sertifikat dari LS-CA yang telah diakreditasi oleh KAN dan memiliki izin operasi dari Menteri Komunikasi dan Informatika berdasarkan pertimbangan dan usulan dari BP-CA;

c) Memiliki jaminan stabilitas finansial dan polis asuransi untuk menutup kewajiban pertanggungjawaban CA;

d) Mengenal dan menguasai bidang transaksi bisnis layanan dengan lingkup dan batas tanggung jawab yang dituangkan dalam CP;

e) Memiliki kompetensi teknis yang dapat dipertanggungjawabkan dan memiliki legalitas serta tanggung jawab hukum;

f) Mempekerjakan personil kompeten, terlatih dan memenuhi kualifikasi, bersertifikat/lisensi untuk kriteria teknis tertentu, menguasai teknis SNI terkait, komunikatif lisan dan tertulis;

g) Mengacu dan menerapkan SNI 19-7125-2005, Teknologi Informasi - Teknik Keamanan - Panduan Teknik untul Penggunaan dan Manajemen Jasa Pihak Ketiga Terpercaya serta ISO/IEC 27001 : 2005, *Information Technology - Security Technique Information Security Management System Requirement.*

---

[131] *Ibid.*, hal.16-17.

Penerbitan Sertifikat Digital[132]

a) Penerbitan SD hanya boleh dilaksanakan oleh CA yang telah memperoleh sertifikat dari LS-CA dan telah mendapatkan izin operasi dari Menteri Komunikasi dan Informatika berdasarkan pertimbangan dan usulan dari BP-CA.

b) Penerbitan SD ini menunjukkan hubungan antara suatu kunci publik kriptografis dengan identitas pelaku transaksi elektronik (sebagai subyek hukum) dan dilakukan sesuai dengan CP, CPS yang ditetapkan oleh CA.

c) CP, CPS dan pelaksanaan penerbitan SD sesuai dengan ketentuan SNI tentang persyaratan CA serta memenuhi semua persyaratan yang ditetapkan oleh BP-CA.

d) Penerbitan SD dilandasi dengan perjanjian antara CA dan pengguna SD, yang mengikat tanggung jawab dan kewajiban masing-masing pihak, serta kepatuhan terhadap peraturan perundang-undangan atau ketentuan lain yang ditetapkan oleh BP-CA.

e) Penerbitan SD meliputi:
   (1) Kegiatan registrast;
   (2) Penerbitan kunci kriptografis;
   (3) Pembuatan dan penandatanganan SD;
   (4) Publikasi SD;
   (5) Pemeliharaan dan pengawasan SD; serta
   (6) Pembekuan sementara atau pembatalan SD.

f) Kegiatan registrasi dilakukan oieh CA untuk mengevaluasi dan meyakini bahwa:
   (1) Data identitas pemohon SD dapat dipercaya dan akurat;
   (2) Pemohon tidak memiliki riwayat melakukan kejahatan transaksi elektronik *(cyber crime);*

[132] *Ibid.*, hal.19-24.

(3) Kegiatan bisnis/perdagangan yang dilakukan oieh pemohon sesuai dengan lingkup jasa CA sebagaimana dinyatakan dalam CP, CPS.

g) Penerbitan kunci kriptografis menggunakan teknik yang telah terbukti aman. Untuk menjamin interoperabilitas dalam berbagai aplikasi bisnis, kunci kriptografis yang diterbitkan agar memenuhi standar yang mengatur persyaratan kemampuan CA yaitu SNI 19-7125-2005, Teknologi Informasi - Teknik Keamanan- Panduan Teknik untuk Penggunaan dan Manajemen Jasa Pihak Ketiga Terpercaya. Sedangkan pengamanan infrastruktur CA persyaratan yang dipenuhi CA adalah ISO/IEC 17799 : 2005, *Information Technology -Security Techniques - Code of Practices For Information Security Management* (Teknologi Informasi – Kode Pengaturan Manajemen Pengamanan Informasi) dan ISO/IE C 27001 : 2005, *Information Technology - Security Technique - Certification Criteria for Information Security Management System - Requirement.* Dalam hal CA tidak menerapkan standar tersebut, dinyatakan dalam CP, CPS. Apabila kunci kriptografis yang dipergunakan diterbitkan oleh pihak lain (misalnya oleh operator infrastruktur kunci publik lain), maka CA harus meyakini bahwa pihak lain tersebut dapat percaya, memenuhi ketentuan di atas, serta mampu memelihara, mengawasi serta melakukan tindakan koreksi apabila temyata kunci kriptografis tersebut tidak cukup aman.

h) Apabila ketentuan tersebut di atas telah dipenuhi, maka CA dapat membuat SD. SD baru dinyatakan sah dan dapat dipublikasi apabila telah ditandatangani oieh pejabat CA yang berwenang.

i) Publikasi SD dapat dilakukan melalui *repository* baik yang disediakan oleh CA sendiri atau oleh pihak lain. CA menjamin agar *repository* yang dipergunakan memiliki sistem pengamanan yang baik sehingga informasi yang di simpan aman dari gangguan.

j) CA memelihara SD dan mengawasi agar informasi yang ada di dalam SD yang diterbitkan tetap akurat dan dapat dipercaya. Pemeliharaan SO termasuk pemutakhiran informasi serta penerapan manajemen pengamanan informasi, pengamanan akses informasi, serta pengamanan fisik dan lingkungan.

Pengawasan akurasi dan kepercayaan informasi termasuk pemantauan akurasi identitas pemegang SD dan penanganan pengaduan, baik dari pemegang SD, dari pihak yang melakukan transaksi dengan pemegang SD, atau dari BP-CA.

k) Pembekuan sementara atau pembatalan SD *(certificate revocation)* dapat dilakukan oleh CA atas permintaan pemegang SD atau karena CA mendapatkan pengaduan tentang :

(1) Penyalahgunaan SD yang diterbitkan; atau

(2) Isi informasi SD mengalami gangguan, dan setelah diselidiki ternyata aduan tersebut benar. Status pembekuan atau pembatalan SD *(revocation status)* harus dipublikasikan baik meialui *repository, WEB* CA atau media publikasi lain;

(3) Kunci pribadi yang berhubungan dengan SD tersebut telah diketahui atau dicurigai telah diketahui oleh pihak lain.

l) Dalam hal SD telah berakhir masa berlakunya, CA dapat mengatur pembaharuan kembali SD. Pengguna SD dapat memperbaharuinya kembali dengan mengajukan permintaan pembaharuan SD kepada CA Apabila pihak pengguna SD tidak memberikan konfirmasi lebih lanjut maka CA dapat melakukan penghentian SD dan dapat berlanjut menjadi penarikan SD, namun CA tetap menjaga semua data dan informasi milik pengguna SD tersebut serta tidak boleh menyebarkan atau mengeluarkan data atau informasi tersebut kepada pihak lain.

m) Penghentian SD dapat dilakukan oleh pengguna SD dengan mengajukan permintaan penghentian kepada CA. Dalam hal ini penghentian SD oleh CA dilakukan dengan persetujuan dari pengguna SD secara tertulis kepada CA dengan alasan yang dapat diterima oleh semua pihak. Penghentian SD dapat berlanjut menjadi penarikan SD jika tidak ada konfirmasi lebih lanjut dari pengguna SD atas permintaan pengguna SD sendiri, atau atas pertimbangan CA. Dalam hal permintaan penarikan SD telah dilaksanakan maka pihak CA segera memberitahukan hal tersebut kepada pengguna SD dan segala hal tersebut di catat dalam *"log book"* yang kemudian dilaporkan kepada otoritas yang berwenang yaitu BP-CA.

n) SD yang kadaluwarsa tidak akan terjadi karena mekanisme yang dibuat tidak memungkinkan adanya suatu SD yang kadaluwarsa. Timbulnya SD yang kadaluwarsa berarti menunjukkan kelemahan dalam sistem CA. Hal ini dapat mengakibatkan diadakannya suatu audit. Sebelum jatuh tempo kadaluwarsa maka pihak CA memberitahukannya kepada pengguna SD. Jika pengguna SD hendak memperpanjang SD nya maka pihak CA mengotorisasi permintaan tersebut dan jika pihak pengguna SD tidak berkehendak untuk memperpanjang SD atau tidak merespon atas pemberitahuan CA, maka tepat pada saat SD tersebut kadaluwarsa, pihak CA segera menarik SD tersebut.

o) Pengaktifan kembali SD yang telah dihentikan dapat dilakukan oleh CA jika ada suatu permintaan dari pengguna SD yang bersangkutan.

Persyaratan Legal Sertifikat Digital

Suatu SD dinyatakan terpercaya jika memenuhi persyaratan sebagai berikut[133]:

c) Data pembuatan SD terkait hanya kepada subyek pembuat SD tersebut saja.

d) Data pembuatan SD pada saat proses pembuatan SD hanya berada dalam kuasa pembuat SD.

e) Segala perubahan terhadap SD yang terjadi setelah waktu pembuatan dapat diketahui.

f) Segala perubahan terhadap informasi elektronik yang terkait dengan SD tersebut setelah waktu pembuatannya dapat diketahui.

g) Terdapat cara tertentu yang di pakai untuk mengtdentifikasi siapa pembuat SD.

h) Terdapat cara tertentu untuk menunjukkan bahwa pemilik SD telah memberikan persetujuan terhadap informasi elektronik yang terkait.

CA memuat dan mencantumkan informasi dan minimal yang harus dipenuhi adalah sebagai berikut[134] :

a) Identitas CA yang menerbitkannya;

---

[133] *Ibid.*, hal.24.

[134] *Ibid.*, hal.24-25.

b) Identitas pemegang atau pemilik atau pelanggan dari SD tersebut;

c) Batas waktu dari masa berlaku atau validitas SD tersebut;

d) Kunci publik dari pemilik SD;

e) Metode yang digunakan untuk mengidentifikasi penandatangan;

f) Hal-hal yang dapat digunakan untuk mengetahui data pembuatan tanda tangan digital.

Keberadaan CA harus diawasi secara intensif karena produk-produk CA memiliki nilai *evidence*. Pengawasan CA diperlukan untuk mendapat kepastian hukum dan melindungi kepentingan masyarakat dari risiko kerugian akibat perbuatan CA yang tidak bertanggung jawab. Terdapat 2 (dua)jenis pengawasan yang harus diiakukan terhadap CA yaitu pengawasan teknis dan pengawasan operasional. Agar pengawasan CA efektif, pengawasan teknis dan pengawasan operasional harus merupakan suatu kesatuan pengawasan yang menyeluruh[135].

a) Pengawasan Teknis[136]

Pengawasan Teknis bersifat preventif, yaitu pelaksanaan penilaian kesesuaian oleh LS-CA untuk membuktikan bahwa suatu CA telah memenuhi persyaratan yang ditetapkan. Penilaian kesesuaian yang dilakukan LS-CA merupakan suatu kombinasi fungsi pengujian dan audit serta evaluasi dan pengambilan keputusan yang diterapkan bagi kategori CA. Produk penilaian kesesuaian ini adalah *Certificate of Conformity* {sertifikat kesesuaian) dan *Mark of Conformity* (tanda kesesuaian). Penilaian kesesuaian mempunyai fungsi seleksi, determinasi, peninjauan dan pengesahan serta pengawasan.

(1) Fungsi seleksi dalam penilaian kesesuaian akan digunakan untuk :

---

[135] *Ibid.*, hal.27.

[136] *Ibid.*, hal.27-29.

(a) Membuktikan kemampuan CA memenuhi persyaratan, antara lain CA sesuai dengan kriteria penilaian CP, CPS, *PKI-Key Management Life Cycle, SD Management Life Cycle,* manajemen operasi CA, dan tanggung jawab organisasi;

(b) Penentuan metode audit serta pengujian fasilitas dan proses pembuatan SD;

(c) Pengumpulan informasi yang relevan untuk pelaksanaan fungsi determination.

(2) Fungsi determinasi dalam penentuan kesesuaian dapat berupa kombinasi sejumlah kegiatan yaitu :

(a) Audit serta pengujian fasilitas dan proses pembuatan SD serta teknologi apraisal teknologi yang dipergunakan;

(b) Pengujian sampel SD;

(c) Audit teknik keamanan teknologi informasi (TI) dan sistem manajemen;

(d) Audit sistem manajemen mutu yang diterapkan pada semua lingkup jasa CA.

(3) Fungsi peninjauan dan pengesahan, yaitu :

(a) Evaluasi semua informasi dan data yang dihasilkan oleh fungsi determinasi;

(b) Pengambilan keputusan;

(c) Penerbitan SD atau tanda kesesuaian;

(4) Fungsi pengawasan diperlukan untuk memastikan bahw CA mampu memelihara dan mengendalikan produk agar tetap sesuai dengan persyaratan serta dapat berupa kombinasi sejumlah kegiatan, tergantung pada skema yang diterapkan, seperti:

(a) Pengujian atau inspeksi sampel SD;

(b) Inspeksi sampel SD yang telah beredar;

(c) Audit dan pengujian ulang fasilitas dan proses pembuatan SD;

(d) Audit Keamanan TI dan Sistem Manajemen Mutu yang diterapkan.

Dalam hal ini fungsi pengawasan tidak perlu dilakukan secara komprehensif sebagaimana saat penilaian awal.

b) Pengawasan Operasional[137]

(1) Pengawasan Operasional (bersifat korektif), yaitu suatu kegiatan pemeriksaan mengenai persyaratan operasional CA. Pengawasan operasional sangat diperlukan untuk mengkoreksi dan menindak CA yang tidak memenuhi persyaratan.

(2) Pengawasan Operasional dilakukan oleh BP-CA.

(3) Tujuan pengawasan BP-CA untuk keperluan :

(a) Mencegah operasi CA yang belum mendapatkan izin operasi dari BP-CA;

(b) Mengawasi penerbitan dan penggunaan SD dari CA yang dinilai oleh LS-CA tidak dapat memelihara kesesuaiannya terhadap ketentuan SNI yang dipersyaratkan atau ternyata digunakan untuk keperluan yang tidak sesuai peruntukannya. BP-CA berwenang meneliti seluruh CA yang terindikasi menyimpang sesuai dengan penilaian LS-CA, untuk kemudian memutuskan sanksi dan menghentikan aktivitas CA.

---

[137] *Ibid.*, hal.29-30.

(4) Pengawasan Operasional yang dilakukan BP-CA sangat penting untuk menegakkan regulasi pasar dan melindungi pengguna CA.

a) Perizinan Operasi CA[138]

Tujuan perizinan operasi CA adalah meningkatkan kepercayaan pelanggan terhadap SD yang dikeluarkan CA dan untuk memberikan kepastian hukum. Izin operasi bagi CA ditetapkan atau dicabut oleh Menteri Komunikasi dan Informatika berdasarkan pertimbangan dan usulan BP-CA.

(1) Untuk memperoleh izin operasi, CA harus sudah memperoleh sertifikat CA dari LS-CA dan mengajukan aplikasi melaiui BP-CA. Pemberian izin operasi kepada CA mengindikasikan kepada masyarakat bahwa CA yang bersangkutan telah memenuhi seluruh persyaratan regulasi, sehingga merupakan CA terpercaya *(trustworthy)*.

(2) Pemohon izin membuktikan telah memiliki sertifikat sebagai CA yang di peroleh dari LS-CA yang terakreditasi oleh KAN.

(3) Pemohon izin membuktikan telah memenuhi persyaratan yang telah ditentukan dan melampirkan:
   (a) Identitas dan status legal;
   (b) CP, CPS;
   (c) *Certificate of Conformity* dari LS-CA.

(4) CA harus menandatangani perjanjian dengan BP-CA yang berisi kewajiban dan liabilitas CA serta kewenangan BP-CA.

(5) Masa berlaku izin operasi CA diberikan untuk jangka waktu tertentu yaitu 3 (tiga) tahun selama memiliki sertifikat dari LS-CA yang berlaku dan dapat diperpanjang untuk jangka waktu yang sama.

b) Perpanjangan Izin Operasi CA[139]

---

[138] *Ibid.*, hal.30-31.

(1) Permohonan perpanjangan izin operasi CA diajukan selambat-lambatnya 3 (tiga) bulan sebelum habisnya masa berlaku izin CA dimaksud.

(2) Perpanjangan izin operasi CA diberikan apabila memiliki sertifikat dari LS-CA yang masih berlaku dan telah memenuhi semua persyaratan yang ditetapkan oleh BP-CA.

e) Pencabutan Izin Operasi CA[140]

Menteri Komunikasi dan Informatika dapat mencabut izin operasi CA berdasarkan pertimbangan dan usulan BP-CA apabila:

(1) CA tidak melaksanakan kewajiban-kewajiban yang telah ditetapkan;

(2) CA menerbitkan SD yang bertentangan dengan ketentuan;

(3) CA atau para pemegang sahamnya dinyatakan pailit;

(4) CA menyalahgunakan izin yang diberikan;

(5) CA tidak dapat melaksanakan kegiatan usahanya sebagaimana tercantum dalam izin yang telah diberikan;

(6) CA melanggar *code of conduct* atau profesionalitas dalam melakukan kegiatan usahanya;

(7) Sertifikat CA yang dimiliki:

(a) Habis masa berlakunya;

(b) Tidak dapat diperpanjang oleh LS-CA;

(c) Dicabut oleh LS-CA.

(8) CA melanggar peraturan perundang-undangan yang berlaku.

f) Penarikan Izin operasi CA[141]

---

[139] *Ibid.*, hal.31.

[140] *Ibid.*, hal.32.

[141] *Ibid.*, hal.32-33.

(1) Penarikan kembali atau penghentian izin operasi CA juga dapat dilakukan atas permintaan dari CA itu sendiri, maka CA berkewajiban :

(a) Mengajukan pemberitahuan tertulis mengenai keinginan pemberhentian izin operasinya kepada BP-CA minimum 3 (tiga) bulan sebelumnya;

(b) Membuat pemberitahuan dan diiklankan, misalnya koran dan media lain, sekurang-kurangnya 3 (tiga) bulan sebelum pemberitahuan tertulis mengenai keinginan pemberhentian izin operasinya.

(2) CA yang berkeinginan untuk memberhentikan izin operasinya wajib mentransfer pelanggannya kepada CA lain yang memiliki izin operasi yang masih berlaku, berdasarkan aturan pengalihan dari BP-CA.

g) Akibat Pencabutan Izin Operasi CA[142]

Pencabutan izin operasi CA berakibat dihentikannya secara langsung hak untuk mengeluarkan SD baru atau memperpanjang yang lama dan tetap melindungi hak para pelanggannya. BP-CA selanjutnya akan mengatur proses pengalihan dan proses-proses lain sebagai akibat dari pencabutan izin operasi CA tersebut.

h) Keberatan dan Upaya Banding[143]

(1) CA dapat mengajukan keberatan terhadap putusan pencabutan izin operasinya kepada Pejabat atau Lembaga yang berwenang untuk meminta suatu putusan yang bersifat final. Permintaan ini harus disampaikan dalam jangka waktu 14 hari sejak dikeluarkannya putusan.

(2) Berdasarkan pengajuan keberatan tersebut, maka Pejabat atau Lembaga yang berwenang akan mengeluarkan putusan yang bersifat final untuk mengabulkan atau menolak keberatan yang diajukan oieh CA dimaksud.

---

[142] *Ibid.*, hal.33.

[143] *Ibid.*, hal.33-34.

Pengamanan Penggunaan CA Pada Transaksi Elektronik

a) Kewajiban Teknis CA[144]

Secara teknis sebuah CA berkewajiban :

(1) Memiliki kerangka legal yang diimplementasikan secara konsisten terhadap semua penggunanya;

(2) Memberikan layanan dasar CA;

(3) Memiliki *policy* yang diimplementasikan dalam CP dar dijabarkan dalam CPS dan kontrak bertangganan;

(4) Dioperasikan dalam kondisi yang memenuhi kaidah-kaidar "keamanan sistem informasi" dan memenuhi standar yang mengatur persyaratan kemampuan teknik yang harus dipenuhi oleh CA yaitu SNI 19-7125-2005, Teknolog Informasi - Teknik Keamanan - Panduan Teknik untuk Penggunaan dan Manajemen Jasa Pihak Ketiga Terpercaya;

(5) Menjelaskan *Certificate Practice Statement* kepada para penggunanya;

(6) Mencatat dan menyimpan semua *record* yang dapat dijadikan sebagai bukti atas layanan yang diberikan;

(7) Merupakan pihak yang independen diantara penggunanya;

(8) Memiliki tanggung jawab atas ketersediaan dan kualitas layanan;

(9) Melakukan audit internal secara berkala.

b) Jaminan Keamanan Dasar CA[145]

Sebagai pihak ketiga terpercaya, CA dapat memberikan jaminan keamanan meliputi :

(1) Memiliki kebijakan keamanan *(Security Policy)* yang memadai;

---

[144] *Ibid.*, hal.35-36.

[145] *Ibid.*, hal.36-37.

(2) Memiliki prosedur dan mekanisme yang dapat mendeteksi jika terjadi masalah keamanan dan mengatasinya dengan menyempumakan prosedur dan mekanisme tersebut;

(3) Memiliki peraturan-peraturan dan tanggung jawab yang dapat menjadi acuan bahwa operasional CA telah dijalankan dengan benar;

(4) Memiliki prosedur dan media untuk berkomunikasi dengan para pengguna;

(5) Menjalankan peraturan dan prosedur secara konstan sesuai dengan level kepercayaan yang telah ditetapkan;

(6) Kualitas dari prosedur operasional dan layanan yang diberikan telah di sertifikasi oleh LS-CA;

(7) Menuangkan dengan jelas hak dan tanggung jawab CA dan penggunaannya dalam kontrak berlangganan;

(8) Memiliki pemahaman yang jelas antara CA denga penggunanya atas tanggung jawab masing-masing pihak;

(9) Sesuai dengan peraturan perundangan yang berlaku;

(10) Telah mengidentifikasikan dengan jelas kemungkinan adanya ancaman keamanan dan cara mengatasinya;

(11) Melakukan penilaian risiko *(Risk Assesment)* secara berkala;

(12) Memiliki organisasi dan sumber daya manusia (SDM) yan sesuai dengan layanan CA dan level kepercayaan yan telah ditetapkan;

(13) Level kepercayaan dari CA dapat diturunkan kepada sebuah Sub CA namun tetap dapat dilakukan proses pengecekan dan klarifikasi;

(14) Kondisi bahwa CA selalu dimonitor dan diawasi oleh BP-C agar tetap sesuai dengan peraturan yang telah ditetapkan.

Peraturan Menteri Komunikasi dan Informatika No. 30 Tahun 2006 tentang Badan Pengawas *Certification Authority*[146]

Dalam Pasal 1 Peraturan Menteri Komunikasi dan Informatika No. 30 Tahun 2006 tentang Badan Pengawas *Certification Authority* disebutkan kedudukan Badan Pengawas *Certification Authority* (BP-CA) adalah lembaga non struktural, yang berada di bawah dan bertanggung jawab kepada Menteri Komunikasi dan Informatika.

BP-CA mempunyai tugas mengawasi, mengendalikan dan berfungsi sebagai *Root CA* serta memberikan pertimbangan dan mengusulkan penerbitan atau pencabutan izin operasi CA kepada Menteri Komunikasi dan Informatika (Pasal 2).

Adapun menurut Pasal 3, fungsi BP-CA adalah sebagai berikut :

1) penyiapan perumusan dan pelaksanaan kebijakan pengorganisasian BP-CA, kebijakan penerbitan dan pencabutan izin operasi CA, kebijakan pembinaan terhadap CA dan Calon CA, kebijakan pengawasan dan pengendalian yang dilakukan oleh BP-CA;

2) pelaksanaan proses untuk menerbitkan izin operasi CA seteiah memiliki sertifikat sebagai CA yang diperoleh dari Lembaga Sertifikasi CA (LS-CA) yang telah diakreditasi oleh Komite Akreditasi Nasional (KAN) atau mencabut izin operasi CA;

3) pemberian pertimbangan dan usulan kepada Menteri Komunikasi dan Informatika dalam menetapkan atau mencabut izin operasi CA;

4) pelaksanaan pengawasan CA, yaitu suatu kegiatan pemeriksaan mengenai persyaratan operasional CA;

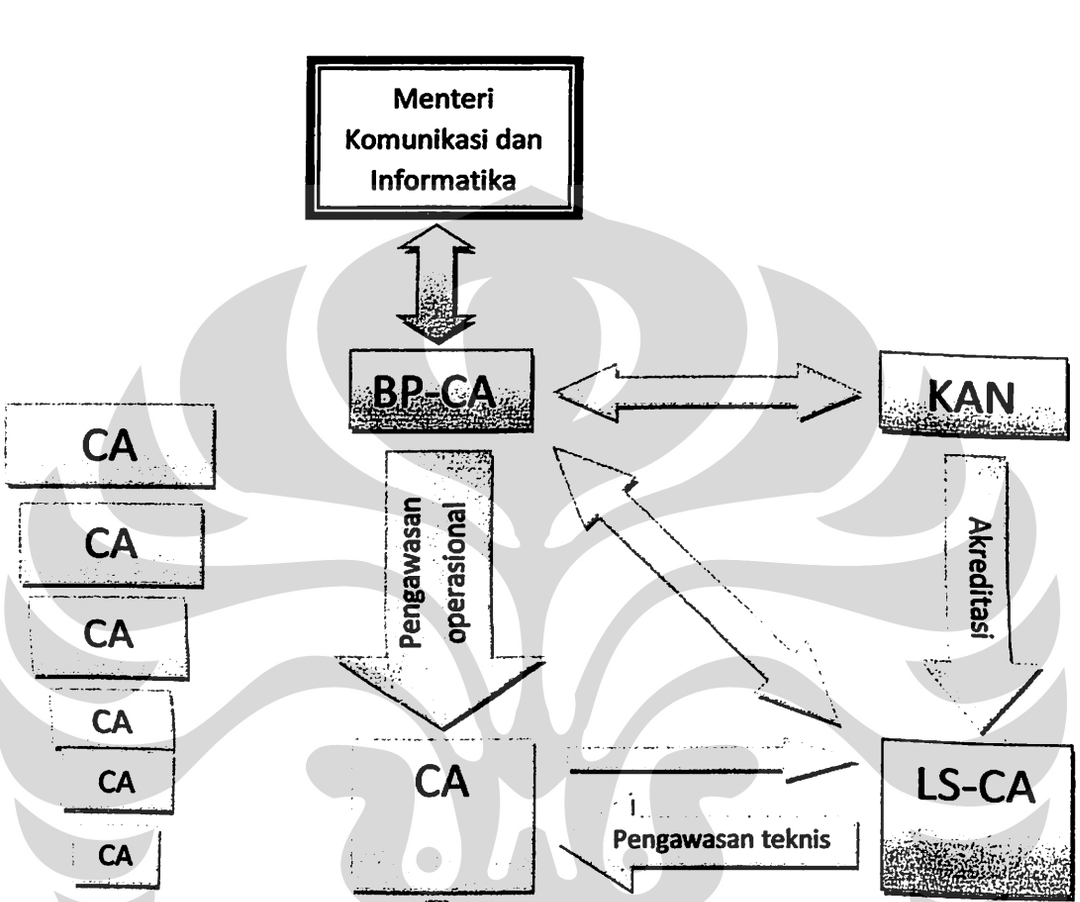
5) pelaksanaan pengendalian untuk mengkoreksi dan menindak CA atau sertifikat digital yang tidak memenuhi persyaratan;

6) pelaksanaan sebagai *Root CA* bagi sertifikat CA.

---

[146] Mulai berlaku sejak ditetapkan di Jakarta pada tanggal 3 Nopember 2006.

Pasal 4 mengatur kewenangan dari BP-CA untuk memverifikasi seluruh CA yang terindikasi menyimpang sesuai dengan penilaian LS-CA namun tetap beroperasi, untuk kemudian memutuskan sanksi dan menghentikan aktivitas CA.



Pengaturan *Certificate Authority* di Indonesia

Gambar 4.1.

UNCITRAL Model Law on Electronic Signatures With Guide to Enactment 2001

Model law ini dibuat untuk melengkapi *UNCITRAL Model Law on Electronic Commerce 1996,* ditujukan untuk menyediakan prinsip-prinsip penting untuk mem-fasilitasi penggunaan tandatangan elektronik. Bagaimanapun, sebagai sebuah "kerangka", *Model Law* tidak mengatur secara rinci (sebagai tambahan kepada kontrak antara para pemakai) juga *Model Law* tidak mengatur seluruh aspek dari penggunaan tandatangan elektronik.

Untuk menghubungkan pasangan kunci dengan tanda tangan prospektif, penyedia layanan sertifikasi (atau otoritas sertifikasi) mengeluarkan sertifikat, catatan elektronik yang merekam daftar kunci publik bersama-sama dengan nama dari pelanggan sertifikat sebagai "subjek" atas sertifikat, dan dapat mengkonfirmasikan bahwa tanda tangan prospektif teridentifikasikan dalam sertifikat berhubungan dengan kunci privat.

Fungsi utama dari sertifikat adalah mengikat kunci publik dengan penandatanganan tertentu. Seorang "penerima" sertifikat mengandalkan tandatangan digital yang diciptakan oleh penandatanganan dalam sertifikat yang dapat menggunakan kunci publik yang terdaftar dalam sertifikat untuk mem-verifikasi bahwa tandatangan digital diciptakan sesuai dengan kunci privat. Jika proses verifikasi sukses, suatu tingkat jaminan disediakan secara teknis bahwa tandatangan digital diciptakan oleh penandatanganan dan bahwa bagian dari pesan menggunakan dalam fungsi *hash* (dan, sebagai akibatnya, pesan data bersesuaian) belum dimodifikasi sejak ditandatangani secara digital[147].

Penyedia layanan sertifikasi secara digital menandatangani SD untuk meyakinkan keaslian dari sertifikat berkenaan dengan isinya dan sumbernya. Tandatangan digital penyedia layanan sertifikasi diverifikasi dengan menggunakan kunci publik dari penyedia layanan sertifikasi yang terdaftar di dalam sertifikat lain oleh penyedia layanan sertifikasi lain (yang dapat, tetapi tidak perlu berada di jenjang yang lebih tinggi), dan sertifikat lain dapat diotentifikasi oleh kunci publik terdaftar di dalam sertifikat lain, sampai seseorang tergantung pada tandatangan digital yang secara pasti terjamin keasliannya. Tandatangan digital juga dapat direkam dalam suatu sertifikat yang dikeluarkan oleh penyedia layanan sertifikasi itu sendiri, dan

[147] *Guide to Enactment UNCITRAL Model Law on Electronic Signatures*, paragraf 53.

kadang-kadang merujuk sebagai sebuah "root CA"[148]. Penyedia layanan sertifikasi harus mengeluarkan secara *digital* sertifikatnya sendiri selama periode operasional penggunaan untuk memverifikasi tandatangan digital penyedia layanan sertifikasi[149].

Otoritas Sertifikasi dapat dioperasikan oleh pemerintah atau oleh penyedia layanan swasta[150].

Unsur-unsur berikut sebagai pertimbangan untuk mengkaji *trustworthiness* suatu penyedia layanan sertifikasi :

1. kemandirian;
2. sumber-sumber daya finansial dan kemampuan finansial untuk menangung resiko dari pertanggungjawaban atas kerugian;
3. keahlian dalam teknologi kunci-publik dan akrab dengan prosedur-prosedur keamanan yang sesuai;
4. umur panjang (otoritas sertifikasi mungkin saja diperlukan untuk menghasilkan bukti dari sertifikasi atau kunci dekripsi bertahun-tahun setelah transaksi selesai, dalam konteks penuntutan perkara atau klaim properti);
5. persetujuan dari perangkat keras dan perangkat lunak;
6. pemeliharaan dari jejak audit dan audit oleh satu entitas independen;
7. adanya suatu rencana darurat (misalnya "pemulihan bencana" perangkat lunak atau kunci *escrow*);
8. pemilihan personil dan manajemen;
9. susunan perlindungan untuk penyedia layanan sertifikasi pemilik kunci privat;
10. keamanan internal;
11. susunan untuk penghentian operasi, mencakup pesan kepada para pemakai;
12. jaminan dan representasi (diberikan atau dikeluarkan);
13. tanggung jawab terbatas;
14. asuransi;
15. *interoperability* dengan otoritas sertifikasi lain; dan
16. prosedur-prosedur penarikan kembali (dalam keadaan dimana kunci kriptografi mungkin saja hilang atau dikompromikan)[151].

---

[148] Catatan Resmi dari Majelis Umum PBB, Sesi Ke-56, Lampiran No. 17 (A/56/17), paragraf. 279.

[149] *Guide to Enactment UNCITRAL Model Law on Electronic Signatures*, paragraf 54.

[150] *Ibid.*, paragraf 58.

Uni Eropa

Penyelenggara Sertifikasi Elektronik atau *Certification Authority* (CA) di Eropa diatur dalam *European Union Directive* 1999/93/EC[152] pada 13 Desember 1999 tentang Tanda Tangan Elektronik.

Tujuan dibuatnya *Directive* ini adalah untuk memfasilitasi penggunaan tandatangan elektronik dan memberi kekuatan hukum dari tandatangan elektronik, member kerangka hukum dari tandatangan elektronik dan penyelenggara sertifikasi, juga tidak mengatur tentang aspek yang berkaitan dengan *validity* kontrak atau kewajiban hukum lainnya dalam hal penggunaan dokumen[153].

Sebelum *Directive* ini dikeluarkan maka *Certification Service Provider* dari suatu negara anggota dari Uni Eropa tidak dimungkinkan untuk memberikan jasa sertifikasi di negara anggota lainnya dari Uni Eropa tanpa meminta ijin terlebih dahulu pada pihak yang berwenang setempat[154].

Dalam Pasal 2 ayat (11) diatur mengenai definisi

"certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures

(terjemahan bebas : CSP adalah entitas atau badan hukum atau orang yang mengeluarkan sertfikat atu menyediakan layanan berkaitan dengan tandatangan elektronik)

Dalam Pasal 2 ayat (13) diatur mengenai definisi

"voluntary accreditation" means any permission, setting out rights and obligations specific to the provision of certification services, to be granted

---

[151] *Ibid.*, paragraf 61.

[152] Dapat dibaca selengkapnya di http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2000%3A013%3A0012%3A0020%3AEN%3APDF.

[153] Pasal 1 *EC Directive* 1999/93/EC

[154] Jos Dumortier,et.al, *The Legal and Market Aspects of Electronic Signatures*, hal.4-5. Lihat di *http://www.ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf*

upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body

(terjemahan bebas : akreditasi sukarela adalah ijin, melaksanakan hak dan kewajiban sesuai ketentuan dari layanan sertifikasi untuk diberikan berdasarkan permohonan dari CSP yang berminat, oleh lembaga privat atua public yang bertugas atau mengawasi dan mempunyai hak dan kewajiban dimana CSP tidak berhak untuk menguji hak dari ijin sampai menerima keputusan dari lembaga tersebut)

Negara anggota tidak diperbolehkan membuat ketentuan bahwa layanan sertifiaksi harus meminta otorisasi lebih dulu[155]. Negara anggota boleh membuat kerangka akreditasi sukarela dimana kerangka tersebut harus bersifat objektif, transparan, proposional dan tidak diskriminatif diskriminatif serta tidak boleh membatasi jumlah CSP[156], tujuan dibuatnya akreditasi sukarela adalah untuk meningkatkan kualitas pelayanan sehingga sesuai dengan *scheme* akreditasi.
Negara anggota akan mendirikan suatu sistem yang mengawasi CSP[157].

Akibat hukum yang dikehendaki dari suatu tanda tangan elektronik berpatokan pada sertifikat yang berkualitas yang dibuat dengan alat pembuat tanda tangan yang aman[158] :

1) memenuhi persyaratan keabsahan tanda tangan dalam hubungan dengan data dalam bentuk elektronik sebagaimana tanda tangan secara tulisan tangan yang memenuhi persyaratan untuk data di atas kertas dan;
2) berkekuatan pembuktian dalam prosedur hukum.

Negara anggota harus memastikan bahwa tanda tangan elektronik tidak akan ditolak keabsahannya sebagai bukti dalam prosedur hukum disebabkan :

1) Dalam bentuk elektronik

---

[155] Pasal 3 ayat (1) *EC Directive*

[156] Pasal 3 ayat (2)

[157] Pasal 3 ayat (3)

[158] Lihat Pasal 5 ayat (1)

2) Tidak berdasarkan sertifikat yang berkualitas
3) Tidak berdasarkan sertifikat yang berkualitas yang dikeluarkan oleh penyelenggara sertfikasi elektronik yang terakreditasi
4) Tidak dibuat dengan alat pembuat tanda tangan yang aman[159]

Tanggung jawab CSP diatur pada Pasal 6 dimana CSP bertanggung jawab untuk memberi ganti kerugian.

Pasal 7 ayat (1) mengatur tentang sertifikat yang dikeluarkan oleh CSP asing berkekuatan hukum sama dengan sertifikat yang dikeluarkan oleh negara-negara anggota Uni Eropa jika:

1) CSP memenuhi persyaratan dalam EC *Directive* dan telah diakreditasi oleh skema akreditasi sukarela di salah satu negara anggota, atau
2) CSP yang berasal dari salah satu negara anggota, atau
3) CSP atau sertifikat tersebut dikenali di bawah perjanjian bilateral atau multilateral antara Uni Eropa dengan Negara ketiga atau organisasi internasional.

Annex I mengatur tentang persyaratan untuk sertifikat yang berkualitas yaitu :

1) indikasi bahwa sertifikat dikeluarkan sebagai sertifikat yang berkualitas;
2) identifikasi CSP dan Negara didirikan;
3) nama penandatangan atau singkatan yang dapat diidentifikasikan;
4) ketentuan hal yang khusus dari penandatangan yang dapat dimasukkan jika dianggap relevan, tergantung tujuan sertifikat itu;
5) verifikasi data tandatangan yang dikorespodenkan untuk pembuatan data tanda tangan di bawah kekuasaan penandatangan;
6) indikasi permulaan dan akhir masa keabsahan sertifikat;
7) kode pengenal sertifikat;
8) tanda tangan elektronik lanjutan dari CSP yang mengeluarkan;
9) pembatasan ruang lingkup penggunaan sertifikat jika dibutuhkan; dan
10) pembatasan nilai transaksi dimana sertifikat dapat digunakan, jika dibutuhkan.

Annex II mengatur tentang persyaratan CSP yang mengeluarkan sertifikat harus:

1) menunjukkan dapat dipercaya untuk menyediakan layanan sertifikasi;

---

[159] Lihat Pasal 5 ayat (2)

2) memastikan operasi dari *prompt* dan direktori yang aman serta keamanan dan pelayanan penarikan yang segera;
3) memastikan tanggal dan waktu ketika sertifikat dikeluarkan atau ditarik dapat digambarkan dengan tepat;
4) memverifikasi , berkoordinasi dengan hukum nasional, identitas dan jika dibutuhkan, ciri-ciri khusus dari orang yang dikeluarkan serifikatnya;
5) memperkerjakan personel yang memiliki keahlian, pengalaman dan kualifikasi yang dibutuhkan untuk menyediakan layanan;
6) menggunakan sistem yang dapat dipercaya dan produk yang dilindungi terhadap modifikasi dan memastikan teknis dan keamanan kriptografi dari ptoses yang mendukungnya;
7) membuat ukuran terhadap pemalsuan sertifikat dam jika CSP mengenerasi pembuatan data tanda tangan menjamin kerahasiaan selama proses tersebut;
8) merawat sumber keuangan untuk beroperasi dengan persyaratan dalam Directive ini, dalam hal risiko tanggung jawab terhadap kerusakan, misalnya dengan mengambil asuransi;
9) merekam semua informasi rekevan sehubungan dengan sertifikat untuk waktu yang tertentu; sehubungan dengan tujuan menyediakan bukti sertifikasi untuk keperluan proses hukum;
10) tidak menyimpan atau menggandakan data pembuatan tanda tangan dari orang yang CSP sediakan layanan pembuatan kunci;
11) sebelum memasuki hubungan kontrak dengan orang yang mencari sertifikat untuk mendukung tandatangan elektronik, informasikan prang tersebut arti dari istilah komunikasi dan kondisi penggunaan sertifikat, termasuk pembatasan penggunaannya, keberadaan skema akreditasi sukarela dan prosedur untuk complain dan penyelesaian perselisihan. Beberapa informasi hars ditransmisikan secara elektronik, ditulis danm dapat dibaca.
12) Menggunakan sistem penyimpanan sertifikat yang terpercaya dalam bentuk : hanya orang yang diberikan kuasa untuk itu dapat membuat perubahan, informasi dapat dicek keasliannya, sertifikat secara public tersedia untuk diperoleh kembali dalam hal mendapat persetujuan dari pemegang sertifikat; dan

13) Perubahan teknis yang mencurigakan keamanan disyaratkan kelihatan oleh operator.

Inggris

Pengaturan mengenai *Certification Authorities* di Inggris terdapat di dalam *Electronic Communications Act* 2000[160] dan *the Electronic Signatures Regulations* 2002 (*the Regulations*)[161], yang berlaku pada tanggal 8 Maret 2002. Ini termasuk ketentuan yang berhubungan dengan tangung jawab dan pengawasan *certification service providers.*

Part I *Section* 1 *Electronic Communications Act* 2000[162] menetapkan suatu tugas pada Sekretaris Negara Bagian/*secretary of state* untuk[163] :

1) memelihara suatu daftar dari penyedia yang disetujui untuk menyediakan layanan pendukung kriptografi, dan mengedepankan sifat alami informasi itu termasuk di dalam daftar;
2) membuat pengaturan untuk mengijinkan anggota dari publik untuk memeriksa isi daftar;

---

[160] *Act* yang mengatur untuk me-fasilitasi penggunaan komunikasi elektronik dan penyimpanan data elektronik; untuk membuat ketentuan tentang perubahan pemberian lisensi di bawah *section* 7 dari Telecommunications Act 1984; dan untuk penggunaan yang berhubungan dengan itu, disetujui pada tanggal 25 Mei 2000. Tersedia di *http://www.bailii.org/uk/legis/num_act/2000/ukpga_20000007_en_1.html* dan *explanatory* notes/penjelasannya tersedia di *http://www.opsi.gov.uk/acts/acts2000/en/ukpgaen_20000007_en_1*

[161] Tersedia di *http://www.legislation.hmso.gov.uk/si/si2002/20020318.htm*

[162] *Register of approved providers*
(1)It shall be the duty of the Secretary of State to establish and maintain a register of approved providers of cryptography support services.
(2)The Secretary of State shall secure that the register contains particulars of every person who is for the time being approved under any arrangements in force under section 2.
(3)The particulars that must be recorded in every entry in the register relating to an approved person are—
(a) the name and address of that person;
(b) the services in respect of which that person is approved; and
(c) the conditions of the approval.
(4)It shall be the duty of the Secretary of State to ensure that such arrangements are in force as he considers appropriate for—
(a) allowing members of the public to inspect the contents of the register; and
(b) securing that such publicity is given to any withdrawal or modification of an approval as will bring it to the attention of persons likely to be interested in it.

[163] Stephen Mason, *Electronic Signatures in Law* (London : LexisNexis UK, 2003), hal. 352.

3) memastikan bahwa perubahan apapun pada daftar adalah untuk diperhatikan oleh mereka yang tertarik pada daftar.

Tujuan dari pendaftaran adalah untuk memastikan penyedia layanan pendukung kriptografi dikaji oleh suatu badan independen mengenai kualitas standar. Hal ini diharapkan akan mendorong penggunaan layanan mereka. Suatu daftar harus ditetapkan, bagaimanapun, penyedia tidak perlu mengajukan permohonan untuk persetujuan, dan mereka mampu untuk menyediakan dukungan pelayanan kriptografi sepanjang dalam keadaan yang normal[164].

Ruang Lingkup dari rejim persetujuan menurut undang-undang

Definisi pendukung layanan kriptografi diatur dalam *Part* I *Section* 6 ECA 2000, yaitu :

(1) "Pendukung layanan kriptografi" berarti layanan apapun yang disediakan untuk pengirim atau penerima komunikasi elektronik, atau pada penyimpanan data elektronik, dan dirancang untuk memberikan fasilitas penggunaan teknik kriptografi dengan maksud untuk :
   (a) mengamankan komunikasi atau data yang mungkin dapat diakses atau mungkin dapat dimasukkan dalam bentuk yang dapat dimengerti, hanya oleh orang tertentu saja; atau
   (b) mengamankan keaslian atau integritas komunikasi atau data yang mempunyai kemungkinan untuk dipastikan[165].

Jenis layanan yang mungkin disetujui di bawah penyusunan adalah layanan dalam hubungan dengan penggunaan kriptografi dengan tujuan untuk :

1) kerahasiaan dan keamanan komunikasi atau data elektronik, sedemikian rupa sehingga hanya mungkin untuk beberapa orang tertentu saja yang dapat

---

[164] Penjelasan / *Explanatory Notes* dari *Electronic Communications Bill*, HL Bill 24-EN 52/3, paragraf 22; diulangi dalam *Explanatory Notes* dari *Electronic Communications Act* 2000, paragraf 22.
The main purpose of the register is to ensure that providers on the register have been independently assessed against particular standards of quality, in order to encourage the use of their services, and hence the development of electronic commerce and electronic communication with Government.

[165] *(1) In this Part "cryptography support service" means any service which is provided to the senders or recipients of electronic communications, or to those storing electronic data, and is designed to facilitate the use of cryptographic techniques for the purpose of—*
(a)securing that such communications or data can be accessed, or can be put into an intelligible form, only by certain persons; or
(b)securing that the authenticity or integrity of such communications or data is capable of being ascertained.

mengakses data dan membuat menjadi bentuk dapat dimengerti, seperti yang diatur dalam *section* 15 ayat (3)[166];

2) menyediakan untuk keaslian atau integritas (keduanya diatur dalam *section* 15(2)[167]) komunikasi atau data elektronik dengan memakai tandatangan elektronik.

ECA 2000 menyediakan penggunaan teknik kriptografi untuk dua tujuan: keamanan dan kerahasiaan data dan tandatangan elektronik. Bagaimanapun perlu dicatat bahwa *Directive* tandatangan elektronik hanya mengacu kepada tandatangan elektronik, tidak pada penggunaan teknik kriptografi untuk keamanan dan kerahasiaan data[168].

Ketentuan dalam *section* 6(2) ECA 2000 membatasi persediaan dari beberapa jenis barang atau layanan tertentu yang berada dalam batasan Undang-Undang ini. *Explanatory Notes* memberikan komentar mengenai *section* 6(2) sebagai berikut:

> (2) Referensi mengenai ketentuan dari layanan pendukung kriptografi tidak meliputi referensi pada penyedia dari atau hak apapun untuk menggunakan perangkat lunak komputer atau perangkat keras komputer kecuali dimana penyedia terhubung kepada ketentuan dari layanan pendukung kriptografi tidak terkandung dalam suatu persediaan[169].

---

[166] *(3) References in this Act to something's being put into an intelligible form include references to its being restored to the condition in which it was before any encryption or similar process was applied to it.*

[167] *(2) In this Act :*

(a)references to the authenticity of any communication or data are references to any one or more of the following :

(i) whether the communication or data comes from a particular person or other source;

(ii) whether it is accurately timed and dated;

(iii) whether it is intended to have legal effect;

and

(b)references to the integrity of any communication or data are references to whether there has been any tampering with or other modification of the communication or data.

[168] Stephen Mason, *ibid.*, hal. 353.

[169] *(2) References in this Part to the provision of a cryptography support service do not include references to the supply of, or of any right to use, computer software or computer hardware except*

Persetujuan skema hanya meliputi layanan dimana ada suatu hubungan berkelanjutan antara penyedia layanan dan pihak *subscribing*/pelanggan. Hal tersebut tidak meliputi hal lain apapun juga, apakah mereka mengambil bentuk perangkat lunak atau perangkat keras, kecuali jika mereka membentuk suatu bagian integral dari layanan. Lebih lanjut, penyedia yang tergolong pada lingkup ini termasuk registrasi/pendaftaran dan sertifikasi dalam hubungan dengan sertifikat, *time-stamping*/mencap-waktu dari sertifikat atau dokumen, *key generation* dan *key management*, *key-storage*/tempat penyimpanan kunci dan ketentuan dari direktori sertifikat[170].

Daftar dari penyedia yang disetujui akan hanya berlaku untuk penyedia layanan jika mereka sedang mengajukan untuk atau sedang menyediakan layanan di Negara Persemakmuran Inggris[171]. ECA mengedepankan kriteria yang menentukan bahwa penyedia dari pendukung layanan kriptografi menyediakan layanan di Inggris, sebagaimana diatur dalam *section* 2(10) bahwa untuk kepentingan pendukung layanan kriptografi yang tersedia di Inggris jika : (pertama) mereka berlokasi di Inggris; (kedua) mereka tersedia untuk seseorang yang berada di Inggris ketika dia menggunakan layanan tersebut; atau (ketiga) mereka disediakan untuk seseorang yang menggunakan layanan untuk kepentingan suatu bisnis yang dilakukan di Inggris atau dari suatu lokasi di Inggris[172].

---

where the supply is integral to the provision of cryptography support services not consisting in such a supply.

[170] *40.Subsection (2) makes it clear that the approval scheme for cryptography support services includes only those services that primarily involve a continuing relationship between the supplier of the service and the customer. The scheme does not cover the supply of an item (whether software or hardware) unless such a supply is integral to the provision of the service itself.*
41. Cryptography support services, falling within the scope of this section, would include registration and certification in relation to certificates, time-stamping of certificates or documents, key generation and management, key-storage and providing directories of certificates.

[171] *Section 2 (1) It shall be the duty of the Secretary of State to secure that there are arrangements in force for granting approvals to persons who :*
(a) are providing cryptography support services in the United Kingdom or are proposing to do so; and
(b) seek approval in respect of any such services that they are providing, or are proposing to provide, whether in the United Kingdom or elsewhere.

[172] *(10)For the purposes of subsection (1) cryptography support services are provided in the United Kingdom if :*
(a) they are provided from premises in the United Kingdom;

Ketentuan dari *section* 2 menugaskan Sekretaris Negara Bagian/*secretary of state* untuk memastikan susunan tersebut pada tempatnya untuk pengabulan persetujuan (*section* 2(1)[173]); apa yang harus dicapai oleh susunan tersebut (*section* 2(2)[174]); dan syarat-syarat yang harus dipenuhi sebelum *secretary of state* akan memberikan persetujuan, dalam arti bahwa orang tersebut :

1) akan mematuhi, dalam menyediakan layanan dengan menghormati yang dietujui, sesuai persyaratan teknis dan persyaratan lain yang mungkin ditentukan;
2) seseorang dalam hubungan dengan siapa yang memenuhi persyaratan lain yang mungkin saja ditentukan, dan akan melanjutkan untuk memenuhi;
3) dan akan melanjutkan untuk, memungkinkan dan berkeinginan untuk mematuhi persyaratan apapun yang diajukan sekretaris negara bagian untuk memaksakan sebagai persyaratan dari persetujuan; dan
4) adalah jika tidak orang yang cocok dan sesuai untuk menyetujui layanan itu[175].

(b) they are provided to a person who is in the United Kingdom when he makes use of the services; or
(c) they are provided to a person who makes use of the services for the purposes of a business carried on in the United Kingdom or from premises in the United Kingdom.

[173] Lihat isi *section* 2(1) di atas

[174] *(2) The arrangements must :*
(a) allow for an approval to be granted either in respect of all the services in respect of which it is sought or in respect of only some of them;
(b) ensure that an approval is granted to a person in respect of any services only if the condition for the grant of an approval to that person is fulfilled in accordance with subsection (3);
(c) provide for an approval granted to any person to have effect subject to such conditions (whether or not connected with the provision of the services in respect of which the approval is granted) as may be contained in the approval;
(d) enable a person to whom the Secretary of State is proposing to grant an approval to refuse it if the proposal is in different terms from the approval which was sought;
(e) make provision for the handling of complaints and disputes which—
(i) are required by the conditions of an approved person's approval to be dealt with in accordance with a procedure maintained by him in pursuance of those conditions; but
(ii) are not disposed of by the application of that procedure;
(f) provide for the modification and withdrawal of approvals.

[175] *(3)The condition that must be fulfilled before an approval is granted to any person is that the Secretary of State is satisfied that the person :*
(a) will comply, in providing the services in respect of which he is approved, with such technical and other requirements as may be prescribed;
(b) is a person in relation to whom such other requirements as may be prescribed are, and will continue to be, satisfied;
(c) is, and will continue to be, able and willing to comply with any requirements that the Secretary of State is proposing to impose by means of conditions of the approval; and
(d) is otherwise a fit and proper person to be approved in respect of those services.

Penjelasan ECA memperkenalkan faktor-faktor relevan untuk memperhitungkan ketika menentukan apakah seseorang cocok dan sesuai, yang meliputi ... pelanggaran apapun yang diatur dalam peraturan ini, dan hukuman untuk pelanggaran termasuk penipuan atau ketidakjujuran, atau melakukan praktek diskriminatif, atau mulai berlaku curang, menekan, praktek bisnis secara tak wajar atau tidak pantas[176].

Ketentuan yang berkenaan dengan suatu rejim persetujuan menurut undang-undang mungkin saja dicabut pada tanggal 25 Mei 2005 jika tidak dibuat berdasarkan *section* 16(2)[177]. Pemerintah telah menyatakan bahwa mereka lebih menyukai untuk mempunyai suatu skema persetujuan sukarela pada tempatnya didukung oleh industri, dan tidak akan mengomentari *Part* I ECA jika mereka sudah puas dengan skema (*tScheme*) yang memenuhi tujuan yang telah mereka tetapkan[178].

Regulasi oleh industri

Badan industri *tScheme* dibentuk pada bulan Mei 2001[179], suatu perseroan terbatas yang dijamin tidak mencari laba, dan secara esensial keanggotaan organisasi diatur oleh seperangkat aturan yang sesudah itu diadopsi di rapat anggota tahunan pada tanggal 9 Mei 2002. Pada saat dilakukannya penulisan ada 19 anggota, 12

---

[176] Lihat *Explanatory Notes* paragraf 28

[177] *16 (2) Part I of this Act and sections 7, 11 and 12 shall come into force on such day as the Secretary of State may by order made by statutory instrument appoint; and different days may be appointed under this subsection for different purposes.*

(4) If no order for bringing Part I of this Act into force has been made under subsection (2) by the end of the period of five years beginning with the day on which this Act is passed, that Part shall, by virtue of this subsection, be repealed at the end of that period.

Section 16(4) menyatakan bahwa *Part* 1 tidak berlaku jika tidak ada suatu perintah yang dibuat ... pada akhir periode dari lima tahun sejak UU ini berlaku.

[178] *10. The Government has said that it would prefer to see an industry led approvals process instead of the statutory scheme envisaged in Part I of the Act. The Alliance for Electronic Business (AEB) has drawn up an industry led scheme (known as the tScheme). The Government has said that it will not commence Part I of the Act if it continues to be satisfied that the tScheme meets the Government's objectives. A prospectus detailing the Scheme has been published and is available at www.fei.org.uk/fei/news/tscheme.html.*

[179] *Articles Association* dan *Memorandum Association* diadopsi pada 23 Januari 2001. Satu salinan dari dokumen ini, demikian pula semua dokumen menunjuk dalam bab ini, dapat diperoleh dari situs *tScheme* pada/di http://www.tscheme.org.

berasal dari organisasi komersial dan 7 dari organisasi nirlaba[180]. Dewan terdiri dari 11 anggota terpilih dan 3 pemakai atau perorangan independen, salah satu diantaranya adalah perwakilan dari pemerintah. Dewan mendelegasikan aktivitasnya kepada panitia kerja, berisikan:

1) Hukum dan Grup Kontrak, yang membuat dan menyelesaikan Model kontrak.
2) Profil dan Komite Proses, terliba dengan mengembangkan *Approval Profiles* dan dokumentasi *Assessment* lain, dan mendefinisikan proses serta prosedur formal.
3) Forum Pemasaran.
4) Komite Persetujuan, bersifat independen dari dewan dan sekretariat dan terdiri dari anggota serta perwakilan pemakai yang bukan anggota dari *tScheme*. Hanya komite ini yang dapat memberi dan menarik kembali persetujuan layanan, walaupun keputusan apapun yang mereka buat berdasarkan pada laporan Assessor.

Organisasi telah memperkenalkan beberapa tujuan:

1) Untuk menyediakan jaminan dengan cara mengembangkan kriteria, dikenal sebagai *Approval Profiles*, dibanding dengan penyedia layanan terpercaya yang dapat dengan bebas dikaji untuk setiap layanan mereka yang diharapkan tersedia untuk klien. Pengkajian independen dilaksanakan oleh assesor yang dikenal tidak sejalan dengan criteria yang terdapat di *Approval Profiles*. *Approval Profiles* dirancang untuk menentukan jika penyedia layanan dengan baik didirikan; mempunyai sumber-sumber daya yang sesuai; layanan yang ditawarkan tergambar dengan jelas; layanan adalah adil dan layak; fungsi layanan sesuai dengan spesifikasi; dan apakah layanan tersebut aman.
2) Untuk menyediakan kontinyuitas dari jaminan. Penyedia layanan kepercayaan dengan puas memenuhi criteria yang diijinkan untuk menggunakan *tScheme Mark* dalam hubungan dengan layanan itu disetujui. Penyedia layanan kepercayaan adalah juga secara kontraktual harus memastikan berlanjutnya praktek yang baik tersebut. *Mark* harus diperbaharui dan dapat ditarik kembali.

---

[180] *Association of Chartered Certified Accountants, APACS, Baltimore Technologies, Barclays Bank, British Chambers of Commerce, BT Ignite, CBI, e-centre, experian, Hitachi, IBM, III (Institute for Information Industries, Taiwan), Intellect, Lloyds-TSB, Microsoft, Office of the e envoy, Royal Mail, The Royal Bank of Scotland Group* dan *Vodafone*

3) Ketentuan dari akreditasi independen dari Lembaga *Assessing* yang pada gilirannya akan diaudit layanan kepercayaan secara elektronik yang ditawarkan oleh penyedia layanan kepercayaan elektronik yang mencari persetujuan *tScheme*.

4) Aplikasi dari kelalaian, dengan upaya untuk mencari ganti-rugi dan memaksakan sanksi berkenaan dengan persetujuan dari penyedia layanan kepercayaan.

Hal tersebut untuk mengantisipasi bahwa skema akan mengganti fungsi pengawasan yang diatur dalam European Directive terhadap tandatangan elektronik[181].

Skema menyetujui suatu kombinasi layanan yang dapat ditawarkan oleh pemohon penyedia layanan kepercayaan. Pendek kata, proses *tScheme* tersebut adalah sebagai berikut:

1) Berbagai *Approval Profiles* telah dikembangkan, diberi hak dan diterbitkan oleh *scheme*.
2) Asesor yang berkualitas diakui oleh suatu organisasi independen skema yang pada gilirannya, melakukan audit sesuai dengan *Approval Profiles*.
3) Pemohon penyedia layanan kepercayaan masuk ke dalam suatu kontrak dengan satu asesor untuk melakukan suatu audit layanannya yang tidak sesuai dengan *profile* yang biasanya atau *profile-profile* lainnya.
4) Pemohon penyedia layanan kepercayaan mengajukan bantuan formal untuk persetujuan kepada *tScheme*.
5) Laporan pengkajian dipertimbangkan oleh *tScheme* dan jika diterima, pemohon penyedia layanan kepercayaan mengadakan suatu kontrak dengan *tScheme* untuk penggunaan *Mark*.
6) Penyedia layanan kepercayaan ditambahkan ke direktori *tScheme* sebagai layanan yang disetujui.

Profil persetujuan (*Approval Profiles*) secara keseluruhan tersedia di dalam file-file Adobe Acrobat pdf dari situs web *tScheme*. Secara ringkas, profil-profil yang digunakan tertera di bawah ini :

1) Profil Persetujuan Dasar (*Base Approval Profile*)

---

[181] Stephen Mason, *ibid.*, hal. 356-357.

Dokumen ini mendefinisikan kriteria dasar dibanding dengan pelamar untuk dikaji agar dapat dipilih sebagai persetujuan. Profil ini digunakan bersama dengan profile persetujuan individu yang dikhususkan untuk jenis tertentu dari layanan yang ditawarkan oleh pelamar. Kriteria dimana pelamar sudah dikaji terdaftar di bawah 'topik pengkajian', dan untuk setiap kriteria topik dimana pengkajian telah dilakukan. Hal ini agar asesor independen dapat merumuskan suatu opini berkenaan dengan kualitas bukti.

Topik pengkajian :

a) Kejujuran bisnis dan kemampuan dari manajemen.
b) Sebuah tinjauan dari kebijakan-kebijakan dan prosedur berkenaan dengan manajemen serta isu keamanan.
c) Pertimbangan dari infrastruktur teknis.
d) Kesesuaian dari personil.
e) Hubungan dengan organisasi eksternal, mencakup komponen layanan dan hubungan yang secara eksternal disediakan dengan pemasok dari teknologi, peralatan dan dukungan pelayanan umum.
f) Kebijakan-kebijakan dan prosedur-prosedur berkenaan dengan penyedia pelayanan.

2) Profil Persetujuan Untuk Layanan Registrasi (*Approval Profile For Registration Services*)

Dokumen ini mendefinisikan kriteria pengkajian untuk pemohon agar dapat terpilih untuk persetujuan dari ketentuan dari layanan kepada individu, objek sistem, entitas korporat dan organisasi lain untuk verifikasi serta registrasi identitas serta atribut lainnya.

Ukuran-ukuran telah di set dalam *Approval Profile* sehubungan dengan ketentuan dari layanan yang mem-verifikasi dan mendaftarkan klaim dibuat oleh pemohon. Terdapat satu lingkup luas untuk mengkaji klaim ini dan kriteria tegas yang tidak dipaksakan.

3) Profil Persetujuan Untuk Penyelenggara Sertifikasi Elektronik (*Approval Profile For Certification Authority*)

Dokumen ini mendefinisikan kriteria pengkajian untuk disetujui sebagai penyelenggara sertifikasi elektronik. Ketika komponen layanan yang

ditawarkan oleh pemohon adalah dikontrakan kepada pihak ketiga, pemohon bertanggungjawab penuh. Dalam keadaan ini, tidak wajib untuk memberitahu publik mengenai hal tersebut, walaupun mungkin hal tersebut dapat dilakukan.

4) Profil Persetujuan Untuk Menandatangani Manajemen Kunci Berpasangan (*Approval Profile For Signing Key Pair Management*)

Dokumen ini mendefinisikan kriteria untuk mengkaji sehubungan dengan ketentuan dari membuat kunci pasangan untuk penggunaan tanda tangan digital. Tingkat dari pengkajian meliputi:

a) Pembuatan (atau ketentuan dari *generating*) menandatangani pribadi dan pasangan kunci tanda tangan publik.

b) Ketentuan dari kunci tanda tangan privat, dimana mereka tidak diberikan atau dikirim ke pelanggan, mencakup perlindungan dan kendali kunci privat.

c) Ketentuan dari kunci publik, dimana mereka tidak diberikan atau dikirim ke pelanggan, dan dimana mereka dikirim ke suatu layanan generasi-sertifikat.

d) Ketetapan kepada pelanggan dari pembuatan tanda tangan menggunakan kunci privat mereka.

e) Susunan untuk penarikan kembali dari satu kunci privat, yang manapun, baik oleh pelanggan atau pemohon otoritas sertifikasi.

5) Profil Persetujuan Untuk Generasi Sertifikat (*Approval Profile For Certificate Generation*)

Dokumen ini mendefinisikan kriteria untuk pengkajian berkenaan dengan persetujuan untuk layanan pembuatan sertifikat.

Persetujuan tertentu yang diandalkan :

a) Layanan untuk registrasi dan verifikasi identitas dari seseorang atau badan hukum berhak atas satu sertifikat, bersama-sama dengan atribut persyaratan apapun (tanggal lahir, alamat, nilai kelayakan pinjam, dan lain-lain) sesuai dengan aturan *Certificate Policy*, seperti yang diatur oleh *Approval Profile* untuk registrasi.

b) Pembuatan kunci kriptografi, sebagaimana diatur oleh *Approval Profiles* untuk *Signing Key Pair Management* dan *Confidentiality Key Pair Management*.

6) Profil Persetujuan Untuk Penyebaran (*Dissemination*) Sertifikat

Dokumen mengedepankan kriteria berkenaan dengan pemenuhan syarat untuk persetujuan menyebarkan sertifikat. Kriteria tersebut mengikuti fungsi berikut:

a) Ketentuan dari sertifikat kepada pelanggan dan jika berdasarkan permintaan atau ijin pelanggan, kepada penerima.

b) Publikasi dari suatu sertifikat dalam suatu tempat penyimpanan untuk diambil kembali.

7) Profil Persetujuan Untuk Manajemen Status Sertifikat

Dokumen ini mendefinisikan kriteria mengenai mengelola status dan kebenaran sertifikat yang meliputi :

a) Penerimaan permintaan untuk menarik kembali, membekukan atau jika tidak mengubah status dari suatu sertifikat.

b) Pengesahan dan otorisasi meminta untuk menarik kembali suatu sertifikat.

c) Berbagai hal yang diperhitungkan ketika membuat suatu keputusan untuk menarik kembali suatu sertifikat, bersama-sama dengan tindakan sehubungan dengan pengambilan suatu keputusan.

d) Pemberitahuan dari suatu perubahan ke status dari suatu sertifikat kepada pihak *subscribing* / pelanggan.

8) Profil Persetujuan Untuk Pengesahan Status Sertifikat

Dokumen yang berhubungan dengan kriteria untuk mengkaji pemohon yang bermaksud menyediakan suatu layanan untuk memverifikasi apakah satu sertifikat adalah sah. Kriteria tersebut diperkenalkan dalam *Approval Profile* yang memperhatikan layanan dengan ketentuan bahwa memungkinkan penerima untuk menentukan kebenaran dari suatu sertifikat di suatu waktu yang tertentu, penerima harus memutuskan untuk menjadi pihak yang memverifikasi. Layanan tersebut meliputi:

c) penawaran akses kepada suatu daftar penarikan kembali sertifikat yang diterbitkan;

d) dengan aktif mendistribusikan daftar;

c) secara langsung mengembalikan status sertifikat kepada *requestor*, misalnya sebagai dengan *On-line Certificate Status Protocol*.

Profil ini terbatas kepada verifikasi dari status suatu sertifikat dan dengan jelas mengeluarkan layanan yang mem-verifikasi tandatangan di sertifikat, menandatangani dokumen atau berkas (*file*)[182].

Proses persetujuan[183] :

1) Pemohon menyiapkan suatu *Specification of Service* kepada *Assessment*. Dokumen ini akan mendefinisikan lingkup dari pengkajian dan mendasari kontrak antara pemohon dan asesor.

   Pelamar memilih asesor yang diakui oleh *tScheme*.

   Pada tahap ini pemohon diharapkan mengajukan pemberian status *Registered Applicant*, dengan mana pelamar memasuki suatu kontrak dengan *tScheme* untuk memperlengkapi suatu jadwal untuk suatu prosedur yang berkenaan dengan pengkajian dan persetujuan layanan. Kontrak ini juga mengikat pemohon kepada *Code of Conduct tScheme*.

2) Pemohon memasuki suatu kontrak terpisah dengan asesor terpilih untuk pengkajian secara terperinci.

   Asesor meninjau bukti yang disediakan oleh pemohon yang tidak sesuai dengan kriteria dalam *Profiles* dan melakukan suatu review terhadap layanan.

   Asesor menyediakan suatu laporan pengkajian kepada pemohon.

   Jika lulus pengkajian maka pemohon kemudian menyampaikan laporan asesor kepada *tScheme*, bersama-sama dengan satu aplikasi formal untuk layanan *approval*.

   Komite *approvals* kemudian akan meninjau laporan dan memutuskan apakah mengabulkan *approval*[184].

Sejalan dengan kerangka dari *Directive* tandatangan elektronik, tScheme mengoperasikan sebuah skema akreditasi sukarela untuk penyedia layanan

---

[182] Stephen Mason, *ibid.*, hal. 357-361.

[183] Selengkapnya dapat dibaca dalam dokumen tScheme "tSd0244 – *Required Assesment Procedures*" yang tersedia di situs tScheme

[184] Stephen Mason, *ibid.*, hal. 361-362.

kepercayaan yang diatur dalam Pasal 3(2)[185] dan 7(l)(a)[186] dari *European Directive* 1999/93/EC. *TScheme* bertujuan untuk mengembangkan hubungan di luar Inggris karena banyak penyedia layanan kepercayaan ingin beroperasi melintasi perbatasan internasional. Untuk melakukan peran ini, *tScheme* bermaksud untuk bekerja sama dengan organisasi sejenis di Eropa dan tempat lain dengan maksud dan harapan untuk memperpanjang kerjasama serta pengenalan timbal balik. Dalam tujuan untuk berintegrasi dengan Eropa, *tScheme* bekerja sama dengan *European Electronic Signature Standardization Initiative* (EESSI) dengan cara aktif terlibat dalam program acara yang relevan, mengenali standar yang diproduksi oleh EESSI, dan mengundang ahli dari EESSI untuk meninjau serta mengomentari *profiles* persetujuan[187].

Amerika Serikat

Pengaturan mengenai *Certification Authorities* di Amerika Serikat terdapat di dalam *Uniform Electronic Transactions Act* (UETA) 1999 dan *the Electronic Signatures in Global and National Commerce Act (E-Sign Act)*,yang pada tanggal 30 Juni 2000 telah ditandatangani oleh Presiden Clinton serta yang mulai berlaku efektif pada tanggal 1 Oktober 2000.

Negara Bagian Washington

---

[185] *2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive.*

Dapat dibaca selengkapnya di *http://209.85.175.104/search?q=cache:VrPj0DTFMc4J:eur-lex.europa.eu/smartapi/cgi/sga_doc%3Fsmartapi!celexapi!prod!CELEXnumdoc%26numdoc%3D31999L0093%26model%3Dguichett%26lg%3Den+European+Directive+1999/93/EC&hl=id&ct=clnk&cd=1&gl=id*

[186] *1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:*

(a)the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or ...

Dapat dibaca selengkapnya di *ibid.*

[187] Stephen Mason, *ibid.*, hal. 362.

Pengaturan mengenai *Certification Authorities* di Negara Bagian Washington terdapat di dalam *Chapter* 19.34. *Electronic Authentication Act* 1997 yang berlaku efektif pada tanggal 1 Januari 1998 dimana peran *secretary of the state* sangat vital.

Singapura

Pengaturan mengenai *Certification Authorities* di Negara Singapura terdapat di dalam *Electronic Transactions Act* yang mulai berlaku 10 Juli 1998. Isi ETA mengikuti *the UNCITRAL Model Law on Electronic Commerce.*

Dalam ETA, pengaturan mengenai CA ada lembaga yang bernama *Controller of Certification Authorities* yang bertugas memberikan ijin/lisensi, sertifikasi dan mengawasi CA[188]. Dalam ETA juga diatur mengenai *scheme voluntary licensing* dari CA[189].

Malaysia

Pengaturan mengenai *Certification Authorities* di Negara Malaysia terdapat di dalam *Digital Signature Act (DSA)* 1997 yang mulai berlaku 1 Oktober 1998. Dalam Part 1 ayat 2 (1) *DSA* mengatur definisi *"certification authority" means a person who issues a certificate* dan *"licensed certification authority" means a certification authority to whom a licence has been issued by the Controller and whose licence is in effect.*

Persyaratan yang harus dipenuhi untuk menjadi CA adalah:

A person intending to carry on or operate as a certification authority must satisfy the following requirements:

a) It is a body corporate incorporated in Malaysia or a partnership within the meaning of the Partnership Act 1961;

b) It maintains a registered office in Malaysia;

c) It has a working capital reasonably sufficient, according to the requirement of the Commission, to enable it to carry on or operate as a certification authority;

d) It files with the Commission a suitable guarantee;

e) It uses a trustworthy system for the generation and management of key pairs and certificates;

f) It uses an approved digital signature scheme for the generation of key pairs and for the creation and verification of digital signatures;

g) It has an operating procedure that includes a certification practice

---

[188] http://www.ida.gov.sg/Policies%20and%20Regulation/20061023155715.aspx

[189] *Ibid.*

statement, the measures to be taken to check the identity of subscribers to be listed in certificates, and the repositories and date/time stamp services to be used;

h) It employs as operative personnel only persons who:

a. Have not been convicted within the past 15 years of an offence involving fraud, false statement or deception; and

b. Have demonstrated knowledge and proficiency in following the requirement of the Act and its Regulations;

i) It complies with the licensing, standards and technical requirements under the Act and its Regulation; and

j) It complies with such other requirement as the Commission thinks fit[190].

Kriteria untuk pengakuan terhadap *Certification Authorities* asing adalah [191]:

a. A foreign certification authority is eligible for recognition if an international treaty, agreement or convention concerning the recognition of its certificates has been concluded to which Malaysia is a party;

b. It must be licensed or otherwise authorized by the relevant governmental entity in that country to carry on or operate as a certification authority in that country;

c. The certificate issued by the foreign certification authority demonstrates a level of security equal to or more stringent than the level of security of a certificate issued by a licensed certification authority in Malaysia;

d. It has established a local agent for service of process in Malaysia;

e. It complies with the standards and technical requirements under the Act and its Regulations; and

f. It complies with such other requirements as the Commission thinks fit Application for the Recognition of a Foreign Certification Authority.

Dalam EU Directive diatur mengenai tingkatan electronic sign, sebagai berikut:

1. Apabila e-sign tersebut berasal dari C.A. di Eropa maka dikatakan sebagai ordinary e-sign

2. Apabila e-sign tersebut sesuai dengan peraturan EU Directive maka e-sign tersebut dikatakan sebagai advanced e-sign

---

[190] *http://www.skmm.gov.my/what_we_do/licensing/dsa/lca.asp*

[191] http://www.skmm.gov.my/what_we_do/licensing/dsa/foreign.asp

3. Apabila e-sign tersebut sesuai dengan peraturan nasional tentang e-sign di salah satu Negara anggota Uni Eropa dimana e-sign tersebut digunakan maka e-sign tersebut dikatakan sebagai certified e-sign

EU dalam Directive 1999/93/EC dan Inggris dalam ECA menganut sistem *voluntary accreditation scheme* diikuti oleh Singapura *voluntary accreditation*, sedangkan Malaysia, Amerika dalam UETA serta Negara Bagian Washington dalam Chapter 19.34 adalah *license*.

Acuan/ *bench marking* untuk membuat peraturan tentang CA adalah *Directive* EU dan *UETA* dari Amerika, tetapi terhadap kedua pengaturan tersebut ternyata masih belum sepenuhnya memberikan perlindungan hukum bagi penguna CA maka dalam rapat pembahasan penyesuaian Permeninfo No. 29 dan 30 Tahun 2006 dengan UU ITE, diusulkan konsep *hybrid*/menggabungkan yaitu :

1. *government* : *licenced* CA

   untuk penggunaan SD di lingkungan pemerintahan maka SD tersebut harus dikeluarkan oleh CA yang berijin operasi/lisensi dari BP-CA.

2. *private* : a) *non-registration*
   b) *registration* : *non accredited* dan *accredited*

   untuk penggunaan SD di lingkungan privat atau di luar pemerintahan maka SD dapat dikeluarkan oleh CA yang tidak terdaftar dan ini biasanya hanya untuk penggunaan terbatas SD di lingkungan tersebut, SD selain itu juga dapat dikeluarkan oleh CA yang terdaftar, baik yang sudah diakreditasi oleh BP-Ca atau belum diakreditasi.

BAB 5

PENUTUP

5.1. KESIMPULAN

1. Semua ketentuan perjanjian dalam KUHPerdata dapat diterapkan pula pada perjanjian dalam transaksi elektronik, sebagai akibat adanya perkembangan ilmu pengetahuan dan teknologi, maka status perjanjian yang diikat dalam transaksi elektronik sah dan mengikat bagi para pihak yang membuatnya. Selain sah menurut hukum perjanjian Indonesia, perjanjian elektronik juga sah menurut konvensi internasional. Sahnya perjanjian elektronik juga harus melihat pada identifikasi para pihak yang membuat perjanjian dengan cara diverifikasi sertfikat elektronik para pihak oleh penyelenggara sertifikasi elektronik.

2. Untuk menjalankan *e-commerce*, dibutuhkan tingkat keamanan yang dapat diterima. *E-commerce* yang menggunakan *internet* relatif bersifat tidak aman, *open* dan memanfaatkan *open system*. Di dunia internet relatif sulit sekali memastikan apakah seseorang itu benar *personal* yang dimaksud sehingga timbul permasalahan mendasar dalam pemanfaatan *e-commerce*. Salah satu cara untuk meningkatkan keamanan dalam *e-commerce* adalah dengan menggunakan teknologi *kriptografi*, yaitu antara lain dengan menggunakan *enkripsi* untuk mengacak data. Salah satu metoda yang mulai umum digunakan adalah pengamanan informasi dengan menggunakan *public key system*. Sistem lain yang bisa digunakan adalah *private key system*. Infrastruktur yang dibentuk oleh sistem public key ini disebut *Public Key Infrastructure* (PKI), atau diterjemahkan dalam Bahasa Indonesia menjadi Infrastruktur Kunci Publik (IKP), dimana kunci publik dapat dikelola untuk pengguna yang tersebar (di seluruh dunia). Salah satu komponen dari infrastruktur kunci publik ini adalah *certification authority* (C.A.) yang merupakan sebuah *body /*

entity yang memberikan dan mengelola sertifikat digital yang dibutuhkan dalam transaksi elektronik. CA berhubungan erat dengan pengelolaan *public key system. Certification/Certificate Authority* (CA) baik berupa perorangan maupun badan hukum yang berfungsi sebagai pihak ketiga (*Trusted third party*) yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik/digital serta menyediakan layanan keamanan yang dapat dipercaya oleh pengguna dalam menjalankan pertukaran informasi secara elektronis dan memenuhi empat aspek keamanan (*Confidentiality; Authentification; Integrity; Non repudiation*). *Certification Authority* (CA) memastikan atau menegaskan identitas seseorang (*subscriber),* dan bertugas menyatakan bahwa kunci publik dari pasangan kunci publik-privat yang digunakan untuk membuat *digital signature* adalah milik orang tersebut. CA akan mengeluarkan suatu sertifikat berbasis komputer (sertifikat digital atau SD) yang menyatakan hubungan antara suatu kunci publik dan *subcriber* yang diidentifikasi. Dalam sertifikat tersebut terdapat kunci publik *subscriber* dan informasi lain yang diperlukan seperti tanggal masa berlakunya kunci publik. Untuk menjamin keaslian dan keutuhan isi sertifikat tersebut, CA membubuhkan *digital signature* CA pada sertifikat.

3. Perbandingan pengaturan penyelenggara sertifikasi elektronik (*certificate authority* atau CA) asing di Uni Eropa (UE) atau *European Union* (EU), Inggris, Amerika, Singapura, Malaysia dan Indonesia

   a. Istilah yang digunakan

      Uni Eropa dalam *EC Directive* 1999/93/EC menggunakan istilah *certification service provider*, *Electronic Communications Act* 2000 dan *the Electronic Signatures Regulations* 2002 (*the Regulations*) dari Negara Inggris Raya menggunakan istilah *cryptography support service* sedangkan Amerika, Singapura, Malaysia dan Pasal 1 butir (10) UU ITE menggunakan istilah Penyelenggara Sertifikasi Elektronik (*certificate authority*).

   b. Bentuk C.A.

Uni Eropa dalam *EC Directive* 1999/93/EC mengatur bahwa C.A. dapat berbentuk entitas, badan hukum dan perorangan, *Electronic Communications Act* 2000 dari Negara Inggris Raya mengatur bahwa C.A. berbentuk perorangan sedang UU ITE Indonesia mengatur bentuk Penyelenggara Sertifikasi Elektronik adalah badan hukum.

c. *Voluntary accreditation schemes*

Uni Eropa dalam *EC Directive* 1999/93/EC mengatur bahwa ada skim akreditasi secara sukarela untuk meningkatkan kualitas dari C.A., , *Electronic Communications Act* 2000 dari Negara Inggris Raya membentuk *accreditation schemes* C.A. yang dinamakan *tscheme* sedang UU ITE Indonesia tidak mengenal skim sukarela ini.

d. *Foreign* CA / CA asing

*C.A.*dalam pasal 13 ayat ke-3 diterangkan harus berbadan hukum dan beroperasional di Indonesia, sehingga lembaga-lembaga C.A. asing seperti Thawte, Verisign dan CaCert.org jika ingin beroperasional di bawah yuridiksi Negara Kesatuan Republik Indonesia harus memiliki akte yang menerangkan badan hukum, terdaftar di Indonesia, dalam hal ini terdaftar di Direktorat Jenderal Aplikasi Telematika di Departemen Komunikasi dan Informatika dan kegiatan operasional CA tersebut benar di Indonesia , tetapi berdasarkan Pasal 54 UU ITE, Peraturan Pemerintah yang disyaratkan dalam pasal-pasal UU ITE ini paling lama 2 (dua) tahun sejak berlakunya UU ini pada tanggal 21 April 2008 harus sudah dibuat, selama belum ada maka berdasarkan ketentuan peralihan di Pasal 53 UU ITE maka peraturan perundang-undang yang lama sepanjang tidak bertentangan dengan UU ini dinyatakan masih berlaku maka untuk peraturan mengenai CA masih dapat digunakan Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2006 tentang Pedoman Penyelenggaraan *Certification Authority* di Indonesia. Dalam Lampiran Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2006 tentang Pedoman Penyelenggaraan *Certification Authority* (CA) di

Indonesia[192] tentang elemen yang harus dimiliki bentuk organisasi CA butir kedua berbunyi " Memiliki peran *cross border,* berarti hukum nasional mengatur keberadaan CA yang ada sebagai subyek hukum di Indonesia dan hukum nasional mengakui eksistensi keberadaan CA internasional yang eksis sesuai hukum tempat domisili CA tersebut; ..." Hal tersebut mengandung arti bahwa status CA asing di Indonesia diakui sah menurut hukum domisili CA tersebut, maka kedudukan CA asing dalam perjanjian antara CA asing dengan *subscriber* diakui cakap/mempunyai kapasitas sesuai hukum domisili CA tersebut.

5.2. SARAN

Hasil penelitian menunjukkan bahwa Indonesia secara mental masih belum siap sedangkan di lain sisi, hal ini sifatnya sangat mendesak. Kalangan masyarakat Indonesia yang selama ini telah melakukan kegiatan dalam ruang lingkup *electronic commerce*, setidak-tidaknya yang mengetahui atau concern mengenai masalah ini hanya terbatas pada kalangan yang selama ini akrab dengan Internet (walaupun telah disebutkan sebelumnya kemungkinan *e-commerce* di luar internet). Sedangkan kalangan ini hanyalah sebagian kecil dari masyarakat. Selain karena pengguna komputer (yang secara tidak langsung berpengaruh) relatif masih sedikit. Dengan perkataan lain, masyarakat Indonesia harus segera menyiapkan diri menghadapi masalah ini sesegera mungkin, mengingat negara lain sudah menyiapkan diri dalam mensikapi perdagangan secara elektronis, dengan adanya kemudahan-kemudahan yang dibawanya. Oleh karena itu, perlu dipikirkan adanya sosialisasi *e-commerce* kepada seluruh masyarakat Indonesia

Kemudian ada masalah, belum siapnya beberapa peraturan hukum Indonesia. Prinsip yang disarankan untuk dipegang adalah *"Transform the Medium, not the Instrument"*. Kegiatan-kegiatan dalam *e-commerce* secara umum masih dapat dikategorikan sebagai tindakan perdagangan/peniagaan biasa, walaupun terdapatnya hal-hal yang signifikan yang membedakannya seperti media elektronik yang menggantikan *paper-based transaction.* Dapat dikatakan beberapa peraturan hukum

[192] Hal.11.

yang telah ada sekarang ini sudah dapat mencukupi, baik dengan cara melakukan penafsiran secara analogis terhadap tindakan yang ada dalam *e-commerce* (terhadap aturan yang belum ada) maupun melakukan penafsiran ekstentif dengan cara memberlakukan peraturan hukum pada hal-hal yang secara esensi adalah sama (contohnya: listrik dan data elektronik).

Dalam hal-hal yang khusus, sangat perlu dibuat peraturan hukum baru, seperti adanya pengaturan khusus di bidang *digital signature* sebagai mekanisme sekuriti utama untuk *e-commerce*, karena dalam bidang ini tidak dapat dilakukan penafsiran untuk menghindarkan kesalahpengertian mengenai esensi dari *digital signature*.

Perlu diperhatikan lebih lanjut bahwa perangkat hukum di Indonesia khususnya hukum perdata pada dasarnya telah mampu menjangkau permasalahan-permasalahan yang timbul. Hukum perdata ini secara umum (secara umum : norma sudah mampu, tetapi Indonesia masih membutuhkan pengaturan yang lebih spesifik untuk menjamin kepastian hukum bagi setiap perbuatan hukum perdata khususnya di bidang *electronic commerce*).

Penelitian ini juga merekomendasikan agar dibentuk suatu tim khusus di bidang hukum/regulasi e-commerce sesegera mungkin. Tim khusus ini perlu segera dibentuk untuk mempersiapkan peraturan hukum di bidang e-commerce khususnya Digital Signature. Kedudukan tim ini di bawah beberapa departemen, seperti Sekretariat Negara, Departemen Perdagangan dan Industri, Departemen Kehakiman, Departemen bidang Telekomunikasi, dan beberapa Departemen lainnya yang berkaitan erat dengan masalah ini. Tim khusus ini dapat bekerja secara inter departemen sehingga segala permasalahan dapat dicakup secara luas.

Bahwa kepastian atas subjek dan objek perdagangan menjadi hal yang diharapkan terkait dengan segala aspek hukumnya, khususnya mengenai legalitas dari suatu perjanjian perdagangan menjadi prosedur resmi adanya formalitas kesepakatan suatu perikatan. Karena transaksi elektronik (*electronic commerce*) secara teknis berbeda karena kemajuan teknologi informatika sehingga perlu diatur mengenai standarisasi teknis yang secara hukum mempunyai kekuatan legalitas yang sama dengan model perjanjian konvensional, baik dalam bentuk

tulisan maupun tanda tangan. Untuk sementara adanya teknologi tanda digital (*digital signature*) yang merupakan prosedur standar teknis dapat menjamin legalitas perjanjian perdagangan dalam transaksi elektronik (*electronic commerce*).

Oleh karena itu, penulis berharap, Peraturan Pemerintah tentang penyelenggaraan sertifikasi tanda tangan elektronik diatur dengan secara mendalam sehingga terjadi keseimbangan antara jaminan integritas dari sebuah akta elektronik dengan jaminan pengidentifikasian Penandatangan, yang pada akhirnya akan memberikan kekuatan hukum, berdasarkan asas praduga kehandalan (*presomption de fiabilité*), kepada tanda tangan elektronik.

DAFTAR REFERENSI

I. BUKU-BUKU

Adolf, Huala. *Hukum Perdagangan Internasional.* Cet.2. Jakarta: PT.Rajagrafindo Persada. 2006.

_____. *Dasar-Dasar Hukum Kontrak Internasional.* Cet.Pertama. Bandung: PT.Refika Aditama. 2007.

Agustina,Rosa. "Undang-Undang Informasi Dan Transaksi Elektronik Dan Hukum Perikatan Internasional", paper dalam Diskusi Ahli dengan Tema "Dinamika Terkini Konvergensi Hukum Telematika Dalam Sistem Hukum Nasional Indonesia", Hotel Ina Kuta,Bali, 12 Juli 2008.

Anonim. Working Group on Electronic Commerce of Japan, *Certification Authority Guidelines version 1.0.* Tokyo:ECOM.1998.

Anson, William R. *Principles of the English Law of Contract,* Oxford: AG Guest University Press, 1961.

Baumer ,David L dan J.C. Poindexter. *Cyberlaw & E-Commerce.* New York : McGraw-Hill. 2002.

Ding,Julian. *E-commerce: Law & Practice.* Kuala Lumpur : Sweet&Maxwell.1999.

Dirdjosisworo, Soedjono. *Kontrak Bisnis (Menurut Sistem Civil Law, Common Law, dan Praktek Dagang Internasional).* Bandung: Mandar Maju.2003.

Endeshaw, Assafa. *Internet dan E-commerce Law with a Focus on Asia Pasific,* Singapore: Prentice Hall, 2001.

Firasa,Roy J. *Cyberlaw : National And International Perspectives.* New Jersey : Prentice Hall. 2002.

Halwani, Hendra. *Ekonomi Internasional & Globalisasi Ekonomi.* Jakarta : Ghalia Indonesia. 2005.

Kantaatmadja , Mieke Komar. (ed.).*Cyberlaw : Suatu Pengantar.* Bandung : ELIPS II.2002.

Kleian , Tommy M. dan Humphrey R. Djemat. *Compendium Hukum Perikatan.* Jakarta: Indonesia Bussiness Law Center. 2006.

Latimer,Paul. *Australian Business Law.*Sydney : CCH Australia Limited. 1998.

Makarim,Edmon. *Pengantar Hukum Telematika (suatu kompilasi kajian)*.Jakarta : PT RajaGrafindo Persada.2005.

Mansur, Dikdik M. Arief dan Elisatris Gultom. *Cyberlaw : Aspek Hukum Teknologi Informasi*. Cet Kesatu. Bandung : PT Refika Aditama. 2005.

Mason, Stephen. *Electronic Signatures in Law*. London : LexisNexis UK. 2003.

Muljadi , Kartini dan Gunawan Widjaja, *Perikatan Yang Lahir dari Perjanjian*. Jakarta:PT RajaGrafindo Persada.2006.

Ramli,Ahmad M. Gunung, Pager., Apriadi, Indra. *Menuju Kepastian Hukum di Bidang Informasi dan Transaksi Elektronik*.Jakarta: Depkominfo RI. Agustus 2006.

Richard Hill dan Ian Walden, *The Draft UNCITRAL Model Law for Electronic Commerce:Issues and Solutions (Teaching Materials)*.1996.

Sanusi, M. Arsyad. *Konvergensi Hukum dan Teknologi Informasi (Sebuah Torehan Empiris – Yuridis)* .Jakarta : The Indonesian Rearch. 2007.

Setiawan,R. *Pokok-Pokok Hukum Perikatan*. Cet.Ketiga. Bandung : Binacipta. 1986.

Smendinghoff,Thomas J. ed. *Online Law: The SPA's Legal Guide To Doing Business On The Internet* .USA: Addison Wesley Developers Press.1996.

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

Subekti dan Tjitrosudibio. *Kitab Undang-undang Hukum Perdata*. terjemahan *Burgerlijk Wetboek* . Jakarta: Pradnya Paramita. 2006.

Subekti. *Aneka Perjanjian*. Cet.VII. Bandung : Alumni. 1985.

_____. *Hukum Perjanjian*. Cet. Ke-20. Jakarta : PT. Intermasa.2004.

Suherman,Ade Maman. *Aspek Hukum Dalam Ekonomi Global*. Cet.Pertama. Jakarta: Ghalia Indonesia. 2002.

Syahrani,Riduan. *Seluk-Beluk Dan Asas-Asas Hukum Perdata*,. Bandung:Alumni. 1992.

Tim Naskah Akademis BPHN. *Naskah Akademis Lokakarya Hukum Perikatan*. Jakarta: Badan Pembinaan Hukum Nasional. 1985.

Vago,Steven. *Law And Society* . New Jersey : Prentice Hall Inc.,1994.

Walden,Ian. *Computer Crime and Digital Investigations*, New Yorks: Oxford University Press Inc., 2007.

Wyasa Putra, Ida Bagus dkk., *Hukum Bisnis Pariwisata* . Bandung:PT. Refika Aditama. 2001.

II. MAJALAH/JURNAL

Badrulzaman,Mariam Darus. *E-Commerce Tinjauan Dari Hukum Kontrak Indonesia* dalam Jurnal Hukum Bisnis, Volume 12. Jakarta : Yayasan Pengembangan Hukum Bisnis.2001.

Gunawan,Johannes. *Reorientasi Hukum Kontrak Di Indonesia* dalam Jurnal Hukum Bisnis, Volume 22, No.6.Jakarta : Yayasan Pengembangan Hukum Bisnis. 2003.

Purbo ,Onno W. "E-Transaction Sulitkan Perbankan", artikel.Jakarta : Biskom, Edisi Mei 2008.

Sjahdeini,Sutan Remy. *E-Commerce Tinjauan Dari Perspektif Hukum* dalam Jurnal Hukum Bisnis, Volume 12. Jakarta : Yayasan Pengembangan Hukum Bisnis.2001.

III. INTERNET

http://209.85.175.104/search?q=cache:_8ROLMFajDEJ:elearning.unej.ac.id/courses/KD225/work/466f560f31aceMengenal_E-com.doc+mengenal+ecommerce&hl=en&ct=clnk&cd=1

http://209.85.175.104/search?q=cache:leWIbdXXpc4J:www.mti.ugm.ac.id/~slamet/kuliah/Aspek_Legal/uu/tugas%2520pak%2520ongkokel%25205/Tugas%2520Aspek%2520Legal%2520-%2520Tinjauan%2520kritis%2520RUU%2520ITE%2520CA.doc+pengaturan+certification+authority+di+amerika&hl=id&ct=clnk&cd=4&gl=id

http://209.85.175.104/search?q=cache:leWIbdXXpc4J:www.mti.ugm.ac.id/~slamet/kuliah/Aspek_Legal/uu/tugas%2520pak%2520ongkokel%25205/Tugas%2520Aspek%2520Legal%2520-%2520Tinjauan%2520kritis%2520RUU%2520ITE%2520CA.doc+hubungan+hukum+antara+ca+dengan+subscriber&hl=id&ct=clnk&cd=2&gl=id

http://209.85.175.104/search?q=cache:s3GTydeEwbEJ:onno.vlsm.org/v01/OnnoWPurbo/contrib/aplikasi/hukum/lokakarya-regulasi-e-commerce-dalam-era-digital-ekonomi-05-20.rtf+pengaturan+certification+authority+di+amerika&hl=id&ct=clnk&cd=2&gl=id

http://209.85.175.104/search?q=cache:VrPj0DTFMc4J:eur-lex.europa.eu/smartapi/cgi/sga_doc%3Fsmartapi!celexapi!prod!CELEXnumdoc%26numdoc%3D31999L0093%26model%3Dguichett%26lg%3Den+European+Directive+1999/93/EC&hl=id&ct=clnk&cd=1&gl=id

http://apps.leg.wa.gov/RCW/default.aspx?cite=19.34

http://budi.insan.co.id/articles/panduan-cyberlaw.pdf

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2000%3A013%3A0012%3A0020%3AEN%3APDF.

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

http://library.usu.ac.id/download/fh/perdata-muhammad.pdf

http://notarisgracegiovani.com/index2.php?option=com_content&do_pdf=1&id=26

http://www.bailii.org/uk/legis/num_act/2000/ukpga_20000007_en_1.html

http://www.bogor.net/idkf/idkf/aplikasi/Copy%20of%20hukum-dan-warfare/mastel-regulasi-2B.doc

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.cert.or.id/~budi/articles/1999-02.pdf

http://www.depkominfo.go.id/portal/?act=detail&mod=program&view=1&id=7

http://www.ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

http://www.elearning.unej.ac.id/courses/KD225/work/466f560f31aceMengenal_E-com.doc

http://www.geocities.com/amwibowo/resource/.htm

http://www.geocities.com/amwibowo/resource/hukum_ttd/hukum_ttd.html

http://www.geocities.com/amwibowo/resource/rut6/laporan.html

http://www.geocities.com/amwibowo/resource/sertifik/tanya.html

http://www.geocities.com/pengacara_rgs/artikel/resume_singkat_hukum_perdata.html

http://www.hukbis.files.wordpress.com/2008/04/e-commerce-ver-2003.ppt

http://www.ida.gov.sg/doc/Policies%20and%20Regulation/Policies_and_Regulation_Level2/Cap%2088%20Rg%201%20(2001)%20Certification%20Authorities%20Regs.JS191206.pdf

http://www.ida.gov.sg/Policies%20and%20Regulation/20060420164343.aspx

http://www.ida.gov.sg/Policies%20and%20Regulation/20060425154627.aspx

http://www.ida.gov.sg/Policies%20and%20Regulation/20060508170238.aspx

http://www.ida.gov.sg/Policies%20and%20Regulation/20061023155715.aspx

http://www.indoregulation.com/

http://www.law.upenn.edu/bll/archives/ulc/fnact99/1990s/ueta99.htm

http://www.law.upenn.edu/bll/archives/ulc/uecicta/ecomemo.txt

http://www.legalitas.org/database/artikel/pidana/esign.pdf

http://www.legalitas.org/database/staatsblad/stb227-1927.pdf

http://www.legalitas.org/database/staatsblad/stb44-1941.pdf

http://www.mcrp.com/ip9-99.pdf

http://www.opsi.gov.uk/acts/acts2000/en/ukpgaen_20000007_en_1

http://www.skmm.gov.my/index.asp

http://www.skmm.gov.my/the_law/ViewLaw.asp?cc=75708200&lg=e&ltrid=2&lrid=62588

http://www.skmm.gov.my/what_we_do/licensing/dsa/datetime.asp

http://www.skmm.gov.my/what_we_do/licensing/dsa/foreign.asp

http://www.skmm.gov.my/what_we_do/licensing/dsa/framework.asp

http://www.skmm.gov.my/what_we_do/licensing/dsa/lca.asp

http://www.skmm.gov.my/what_we_do/licensing/dsa/repository.asp

http://www.solusihukum.com/artikel/artikel8.php

http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

http://www.uncitral.org/pdf/english/uncitral-leaflet-e.pdf

http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html

www.bogor.net/idkf/idkf/aplikasi/Copy%20of%20hukum-dan-warfare/mastel-regulasi-2B.doc

www.cert.or.id/~budi/courses/ec7010/dikmenjur/iqbal-report-2.pdf

www.fei.org.uk/fei/news/tscheme.html.

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

www.wikipedia.org

IV. PERATURAN PERUNDANG-UNDANGAN

KONVENSI INTERNASIONAL

United Nations Convention in Contracts for International Sale of Goods (UNCISG)

UNCITRAL *Model Law on Electronic Commerce*

United Nations Convention on the Use of Electronic Communications in International Contracts 2005

UNCITRAL Model Law on Electronic Signatures With Guide to Enactment 2001

UNI EROPA

European Union Directive 1999/93/EC on *Electronic Signatures*

INGGRIS RAYA

Electronic Communications Act 2000

Electronic Signatures Regulations 2002 *(the Regulations)*

AMERIKA SERIKAT

*The National Conference of Commissioners on Uniform State Laws (NCCUSL). The Uniform Electronic Transactions Act (UETA)*1999.

The Washington Electronic Authentication Act 1997 or *The* Washington *Digital Signature Act*, RCW 19.34.

SINGAPURA

Electronic Transactions Act

MALAYSIA

Digital Signature Act (DSA)

INDONESIA

Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek), siterjemahkan oleh R. Subekti dan R. Tjitrosudibio, Cet. Ke-37, Jakarta:Pradnya Paramita. 2006.

Reglemen Acara Hukum Untuk Daerah Luar Jawa dan Madura (*Reglement Tot Regeling Van Het Rechtswezen In De Gewesten Buiten Java En Madura*) (*RBg*). *Staatsblad 1927* Nomor *227.*

Reglemen Indonesia Yang Diperbarui (*Het Herziene Indonesisch Reglement*) (*HIR*). *Staatsblad* 1941 Nomor 44.

Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42, Tambahan Lembaran Negara Republik Indonesia Nomor 3821)

Undang-Undang No. 30 Tahun 2004 Tentang Jabatan Notaris (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 117, Tambahan Lembaran Negara Republik Indonesia Nomor 4432)

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843)

Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2006 tentang Pedoman Penyelenggaraan *Certification Authority* di Indonesia

Peraturan Menteri Komunikasi dan Informatika No. 30 Tahun 2006 tentang Badan Pengawas *Certification Authority*

Lampiran Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2006 tentang Pedoman Penyelenggaraan *Certification Authority* di Indonesia