# Tinjauan Kritis Atas CA (Certificate/Certification Authority) dalam UU ITE: Persfektif Akademis

**Dedy Cahyadi***

*Program Studi Ilmu Komputer, FMIPA Universitas Mulawarman*
*Jl. Barong Tongkok no.5 Kampus Unmul Gn. Kelua Sempaja Samarinda 75119*

## Abstrak

Perkembangan internet sebagai salah satu media infromasi dan komunikasi, menjadikan pertukaran informasi atau transaksi data merupakan hal yang umum terjadi termasuk hal yang negatif. CA merupakan lembaga yang mengatur berbagai regulasi kepercayaan di dalam transaksi elektronik. Sertifikat keandalan seperti yang di atur dalam Pasal 10 UU ITE, merupakan kebutuhan pasar yang biasanya terbentuk dengan sendirinya atas permintaan pasar berupa lembaga non pemerintah (swasta) serta pemberdayaan YLKI (non pemerintah) dan Badan Perlindungan Konsumen Nasional (pemerintah) bisa di buat menjadi CA dengan mengikuti aturan-aturan internasional akan pembentukan CA. Semua transaksi yang bernilai komersil terjadi di internet yang melibatkan kedua belah pihak memerlukan pihak ke tiga (*Trusted third party*) atau CA sebagai jembatan kepercayaan dan aspek legalitas kedua belah pihak yang bertransaksi, termasuk transaksi yang melibatkan pihak perbankan, atau institusi keuangan lainnya. UU ITE belum menjabarkan peraturan penyelenggara sertifikasi atau CA sehingga diperlukan peraturan lain sebagai persyaratan pelaksanaan pasal 12,13 dan 14 dalam UU ITE, namun di beberapa hukum nasional dan internasional pelaksanaan CA bisa dilakukan dengan mengambil persamaan materi muatan hukum.

**Kata kunci :** Undang-undang, Transaksi Elektronis, Informasi, Cyberlaw, Certification Authority, Certificate Authority

## I. Pendahuluan

Pada Januari 1960, J.C.R. Licklider menuangkan ide pertama kali tentang internet ke dalam papernya, *Man-Computer Symbiosis.* Kemudian Oktober 1962, DARPA mengangkat Licklider sebagai kepala riset computer yang salah satu risetnya menghubungkan tiga komputer yaitu System Development Corporation di Santa Monica, University of California, Berkeley dan MIT. Dan terus berkembang yang akhirnya di sebut ARPANET, dari ARPANET lahir berbagai standar interkoneksi salah satunya TCP/IP yang menghubungkan jaringan komputer pada saat ini, atau di kenal dengan istilah internet.

Walau Indonesia termasuk ke dalam negara yang lambat pertumbuhan internetnya, namun masih merupakan pasar yang potensial di kawasan Asia tenggara karena jumlah penduduknya terbesar, sehingga akan di prediksikan memiliki pertumbuhan pengguna internet yang besar pula.

Seiring dengan perkembangan internet sebagai salah satu media infromasi dan komunikasi, maka pertukaran informasi atau transaksi data merupakan hal yang umum terjadi termasuk hal yang negatif terhadap penggunaan internet seperti kasus Clearing BRI Yogyakarta (25 Juni 1984) merupakan kasus yang pertama kejahatan melalui komputer di bawa ke mahkamah agung (Harris, 2007), kemudian pembobolan situs KPU, kasus Klik BCA sampai dengan Redirecting DNS situs resmi presiden Susilo Bambang Yudhoyono.

## II. Regulasi Internasional tentang CA (Certificate Authority)

### 2.1. Perlunya CA sebagai *Trusted third party*

CA atau Certification / Certificate Authority merupakan sebuah 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 elektonis dan memenuhi 4 aspek keamanan (*Confidentiality; Authentification; Integrity; Non repudiation*) (Ramli, 2006).

CA berkedudukan sebagai pihak ketiga yang dipercaya untuk memberikan kepastian/pengesahan terhadap identitas dari seseorang/pelanggan (klien CA tersebut). Selain itu CA juga mengesahkan pasangan kunci publik dan kunci privat milik orang tersebut. Proses sertifikasi untuk mendapatkan pengesahan dari CA dapat dibagi menjadi 3 tahap:

1. Pelanggan/*subscriber* membuat sendiri pasangan kunci privat dan kunci

* e-mail : dedy.cahyadi@gmail.com

publiknya dengan menggunakan software yang ada di dalam komputernya
2. Menunjukan bukti-bukti identitas dirinya sesuai dengan yang disyaratkan CA
3. Membuktikan bahwa dia mempunyai kunci privat yang dapat dipasangkan dengan kunci publik tanpa harus memperlihatkan kunci privatnya.

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

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

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

1. Identitas CA yang menerbitkannya.
2. Pemegang/pemilik/*subscriber* dari sertifikat tersebut.
3. Batas waktu keberlakuan sertifikat tersebut.
4. Kunci publik dari pemilik sertifikat.

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

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

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

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

1. Penjual (*merchant*)
2. Pembeli (*buyer*)
3. Certification Authority (CA)

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

4. *Account Issuer* (penerbit rekening contoh: kartu kredit)
5. Jaringan pembayaran (contohnya Visa dan Mastercard)
6. Internet Service Provider (ISP)
7. Internet *Backbone*

Perusahaan atau lembaga CA yang basa digunakan di internet antara lain, VeriSign, Thawte, GeoTrust, Comodo, CaCert.org.

### 2.2. Instrumen Hukum Internasional

Instrumen Hukum Internasional di bidang kejahatan cyber (Cyber Crime) merupakan sebuah fenomena baru dalam tatanan Hukum Internasional modern mengingat kejahatan cyber sebelumnya tidak mendapat perhatian negara-negara sebagai subjek Hukum Internasional. Dimana terdapat tiga yuridiksi hukum internasional (Ramli, 2006), yaitu:

1. Yurisdiksi menetapkan undang-undang (*the jurisdiction of prescribe*);
2. Yurisdiksi penegakan hukum (*the jurisdiction to enforcve*);
3. Yurisdiksi menuntut (*the jurisdiction to adjudicate*).

Munculnya bentuk kejahatan baru yang tidak saja bersifat lintas batas (transnasional) tetapi juga berwujud dalam tindakan-tindakan virtual telah menyadarkan masyarakat internasional tentang perlunya perangkat Hukum Internasional baru yang dapat digunakan sebagai kaidah hukum

internasional dalam mengatasi kasus-kasus Cybercrime.

2.2.1. Uni Eropa

Instrumen Hukum Internasional publik yang mengatur masalah Kejatan cyber yang saat ini paling mendapat perhatian adalah Konvensi tentang Kejahatan cyber (Convention on Cyber Crime) 2001 yang digagas oleh Uni Eropa (Mursito, Sirait & Wardhana, 2005). Konvensi ini meskipun pada awalnya dibuat oleh organisasi Regional Eropa, tetapi dalam perkembangannya dimungkinkan untuk diratifikasi dan diakses oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan Cyber.

Negara-negara yang tergabung dalam Uni Eropa (Council of Europe) pada tanggal 23 November 2001 di kota Budapest, Hongaria telah membuat dan menyepakati Convention on Cybercrime yang kemudian dimasukkan dalam European Treaty Series dengan Nomor 185. Konvensi ini akan berlaku secara efektif setelah diratifikasi oleh minimal 5 (lima) negara, termasuk paling tidak ratifikasi yang dilakukan oleh 3 (tiga) negara anggota Council of Europe. Substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan kriminal (criminal policy) yang bertujuan untuk melindungi masyarakat dari cyber crime, baik melalui undang-undang maupun kerjasama internasional.

Hal ini dilakukan dengan penuh kesadaran sehubungan dengan semakin meningkatnya intensitas digitalisasi, konvergensi, dan globalisasi yang berkelanjutan dari teknologi informasi, yang menurut pengalaman dapat juga digunakan untuk melakukan tindak pidana. Konvensi ini dibentuk dengan pertimbangan-pertimbangan antara lain sebagai berikut : Pertama, bahwa masyarakat internasional menyadari perlunya kerjasama antar Negara dan Industri dalam memerangi kejahatan cyber dan adanya kebutuhan untuk melindungi kepentingan yang sah dalam penggunaan dan pengembangan teknologi informasi.

Kedua, Konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. Hal lain yang diperlukan adalah adanya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat.

Ketiga, saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk Perlindungan Hak Azasi Manusia dan Konvenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik Dan sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekspresi, yang mencakup kebebasan untuk mencari, menerima dan menyebarkan informasi/pendapat.

Konvensi ini telah disepakati oleh Masyarakat Uni Eropa sebagai konvensi yang terbuka untuk diakses oleh negara manapun di dunia. Hal ini dimaksudkan untuk dijadikan norma dan instrumen Hukum Internasional dalam mengatasi kejahatan cyber, tanpa mengurangi kesempatan setiap individu untuk tetap dapat mengembangkan kreativitasnya dalam pengembangan teknologi informasi.

2.2.2. United Nations in Contracts for International Sale of Goods (UNCSIG)

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 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 di adopsi. Konsepsi yang bisa diambil dari konvensi ini antara lain adalah:

1. 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(negara bagian Utah, California), Malaysia, Singapura.

2. 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 kewaarganegaranya. 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.

3. 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 dialukan tanpa kehadiran para pelaku di satu tampat (beetwen absent person). CISG memberikan kepastian di dunia perdagangan internasional mengenai saat terjaadinya 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 kelambatan(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).

2.2.3. Kontrak berdasarkan UNCITRAL model law on Electronic Commerce

Model hukum 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 hukum ini mengatur juga tentang *carriage of goods*.

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 messaages apapun bentuk atau formatnya tidak dapat dikatakan tidak mempunayai 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* 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:

1. terdapat suatu metode yang digunakan untuk mengidentifikasi keberadaan seseorang dan juga dapat

mengindikasikan didalam dokumen tersebut telah mendapat persetujuan dari orang tersebut.

2. 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.

2.2.4. UNCITRAL, Draft on Electronic Signature

Draft ini berisi bagaimana suatu data messages dapat ditandatangani secara elektronis. Sebenarnya terminologi Electronic Signature yang dipakai dalam draft ini adalah sama dengan digiatl signnature, namun pihak UNCITRAL memilih terminologi ini mungkin karena medium yang dipakai dalam menandatangani suatu data messages adalah secara elektronik.

Berdasarkan aturan-aturan yang berlaku secara internasional seperti disebut diatas, maka keberadaan *digital signature* (dan berbagai macam istilah lain yang sebenarnya mempunyai maksud yang sama) dalam kontrak perdagangan internasional adalah hampir menjadi semacam standar bagi perdagangan internasional dimasa yang akan datang. Keberadaan *digital signature* pada saat ini dalam penggunaannya sebagai salah satu bentuk kontrak perdagangan internsional telah mempunyai kekuatan hukum. Ia secara hukum mengikat (*legally binding*), meskipun belum ada konvensi yang mengaturnya secara tersendiri.

2.2.5. GUIDEC (General Usage for International Digitally Ensured Commerce) dari ICC

GUIDEC adalah suatu panduan yang dibuat oleh International Chamber of Commerce bagi penggunaan suatu metode yang akan menjamin (*ensured*) keberadaan suatu dokumen/data elektronis dalam penggunaannya dalam dunia internasional. Panduan ini menggunakan terminologi ensured untuk membedakannya dengan terminologi sign dalam hal panandatanganan (*sign in/signature*) terhadap suatu dokumen.

GUIDEC ini dimaksudkan untuk menunjang perkembangan dari e-commerce dengan memberikan kepastian bagi penerapan adanya tandatangan dalam suatu dokumen elektronis. Panduan ini akan menjelaskan berbagai terminologi/istilah yang ada didalam UNCITRAL model law on e-commerce seperti apakah sebenarnya maksud dari penandatangan suatu pesan secara elektronis (*electronically signed Messages*). Maksud dari penandatanganan disini adalah bukan dilakukan secara fisik, tetapi membutuhkan suatu perangkat elektronik.

Terminologi dari *electronically signed* yang dipakai dalam GUIDEC ini adalah penggunaan teknik enkripsi dengan menggunakan kunci publik yang lebih dikenal sebagai *digital signature*. Penggunaan *digital signature* ini akan memberikan kepastian akan keamanan, keutuhan dari data messages yang digunakan dalam e-commerce. Faktor keamanan dan keutuhan dari suatu data messages adalah suatu hal yang sangat menentukan dalam menunjang perkembangan e-commerce. E-commerce yang dilakukan melalui media internet yang merupakan suatu jaringan publik akan memberikan berbagai ketidakpastian bagi para penggunaanya. Dengan adanya suatu panduan mengenai bagaimana suatu data messages dapat dijamin keamanan dan keutuhan melalui cara *digital signature.*

## III. Regulasi Nasional tentang CA

### 3.1. KUHP

Dalam perspektif hukum, suatu perikatan adalah suatu hubungan hukum antara subyek hukum dimana satu pihak berkewajiban atas suatu prestasi sedangkan pihak yang lain berhak atas prestasi tersebut (Wibowo dkk, 1999).

Berdasarkan pasal 1233 KUHPerdata., adanya suatu perikatan adalah lahir karena suatu perjanjian atau karena suatu undang-undang. Selanjutnya, dalam pasal 1320 KUHPerdata. dijelaskan bahwa syarat-syarat sah-nya suatu perjanjian adalah meliputi Syarat Subyektif dan Syarat Obyektif.

Syarat Subyektif meliputi adanya (1) Kesepakatan, dan (2) Kecakapan (bersikap tindak dalam hukum) untuk membuat suatu perikatan. Sedangkan syarat obyektif, adalah meliputi (3) suatu hal yang tertentu (obyeknya harus jelas), dan (4) merupakan suatu kausa yang halal (tidak bertentangan dengan undang-undang, kesusilaan dan ketertiban umum).

Berkenaan dengan syarat subyektif tersebut, diketahui bahwa subyek hukum yang terlibat dalam sistem sekuriti yang menggunakan *digital signature*, antara lain :

1. Pemegang Digital Certificate
2. Certification Autorithies sebagai *issuer* dari Digital Certificate

### 3.2. UU ITE

Pasal – pasal yang memuat tentang CA dan hal-hal yang terkait dengan CA (Anonymous, 2008) antara lain:

1. Pasal 1, memuat pengertian tentang sertifikat elektronik, lembaga sertifikasi keandalan *(trustmark)* dan penyelenggara sertifikasi elektronik
2. Pasal 10, memuat tentang fungsi lembaga sertifikasi keandalan *(trustmark)*
3. Pasal 13 dan 14, memuat peyelenggaraan dan kewajiban dari badan sertifikasi elektronik

Lembaga Sertifikasi Keandalan yang tercantum dalam pasal 10 dapat di bentuk oleh pemerintah maupun masyarakat, lembaga ini juga terkait erat dalam UU perlindungan konsumen serta lembaga sejenis seperti YLKI dan Badan Perlindungan Konsumen Nasional

CA dalam pasal 13 ayat ke-3 diterangkan harus berbadan hukum dan beroperasional di Indonesia, sehingga lembaga-lembaga CA seperti Thawte, Verisign dan CaCert.org jika ingin beroperasional atau website di bawah yuridiksi Negara Kesatuan Republik Indonesia harus memiliki akte yang menerangkan badan hukum dan kegiatan operasional CA tersebut benar di Indonesia

### 3.3. Undang-undang perlindungan konsumen

Berdasarkan Undang-Undang No 8 Tahun 1999 tentang Perlindungan Konsumen yang mulai berlaku satu bulan sejak pengggundangannya, yaitu 20 April 1999. Pasal 1 butir 2 mendefinisikan konsumen sebagai "Setiap orang pemakai barang dan/atau jasa yang tersedia dalam masyarakat, baik bagi kepentingaan diri sendiri, keluarga, orang lain, maupun mahluk hidup lain dan tidak untuk diperdagangkan."

#### 3.3.1. Aspek Hukum Perlindungan Konsumen

Hak-hak konsumen menurut UU No 8 tahun 1999 , dalam Pasal 4 sebagai berikut:

1. Hak atas kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang dan/atau jasa.
2. Hak untuk memilih barang dan/atau jasa serta mendapatkan barang dan/atau jasa tersebut sesuai dengan nilai tukar dan kondisi serta jaminan yang dijanjikan.
3. Hak atas informasi yang benar, jelas dan jujur mengenai kondisi dan jaminan barang dan/atau jasa.
4. Hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan.
5. Hak untuk mendapatkan advokasi, perlindungan, dan upaya penyelesaian sengketa perlindungan konsumen secara patut
6. Hak untuk mendapat pembinaan dan pendidikan konsumen.
7. Hak untuk diperlakukan atau dilayani secara benar dan jujur serta tidak diskriminatif
8. Hak untuk mendapat kompensasi, ganti rugi dan/atau penggantian, apabila barang dan/atau jasa yang diterima tidak sesuai dengan perjanjian atau tidak sebagaimana mestinya.
9. Hak-hak yang diatur dalam ketentuan peraturan perundang-undangan lainnya.

Selain itu terdapat juga kewajiban dari konsumen yang tertera dalam pasal 5 UU no 8 tahun 1999.

Dalam pasal 4 poin ke-3 di atas berkaitan dengan hukum cyber dimana hak dan informasi harus diberikan kepada konsumen melalui media online yang perlindungan atas hak ini antara lain dapat pula diberikan melalui sertifikasi ke andalan *(trustmark)* (Ramli, 2006), yang biasanya di keluarkan oleh lembaga atau organisasi CA Namun di Indonesia hal ini bisa saja di berikan oleh beberapa badan perlindungan konsumen seperti YLKI dan Badan Perlindungan Konsumen Nasional

#### 3.3.2. Aspek Perlindungan konsumen dalam Penggunaan *Digital signature* & CA

Dalam penggunaan *Digital signature* kita mengenal adanya dua pihak, yaitu:

1. Certificate Authority (CA)
2. *Subscriber*

Hubungan ini menunjukkan kaitan antara CA sebagai penyelenggara jasa dan *subscriber* sebagai konsumen. Sebagai penyelenggara jasa, CA harus menjamin hak-hak subsscriber antara lain:

1. Privacy

Termaktub dalam pasal 4 butir 1 UU NO 8 tahun 1999. Contoh: Ketika *subscriber* meng"apply" kepada CA, subs akan dimintai keterangan mengenai identitasnya, besar kecilnya keakuratan dari identitas tersebut tergantung dari jenis

tingkatan sertifikat tersebut. Semakin tinggi tingkat sertifikat maka semakin akurat pula identitas sebenarnya dari *subscriber*.

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

2. Accuracy

Termaktub dalam pasal 4 butir 2,3, dan 8 UU No 8 tahun 1999. Dalam prinsip ini terkandung pengertian "ketepatan" antara apa yang diminta dengan apa yang didapatkan. Bahwa apa yang didapat oleh *subscriber* sesuai dengan apa yang ia minta berdasarkan informasi yang diterimanya. Ketepatan informasi (informasi yang benar tanpa tipuan) juga merupakan prinsip accuracy.

Sebagai contoh: *subscriber* yang meminta level tertentu dari sertifikat sebaiknya tidak diberikan level yang lebih rendah atau lebih tinggi.

CA juga berkewajiban memberitahukan segala keterangan yang berkaitan dengan penawaran maupun permintaan yang diajukan.

3. Property

Termaktub dalam pasal 4 butir 8 UU No 8 tahun 1999. *Subscriber* harus dilindungi hak miliknya dari segala penyimpangan yang mungkin terjadi akibat masuknya *subscriber* ke dalam sistem ini. Artinya *subscriber* berhak dilindungi dari segala bentuk penyadapan, penggandaan, dan pencurian. Jika hal ini terjadi maka CA berkewajiban mengganti kerugian yang diderita.

4. Accessibility

Termaktub dalam pasal 4 butir 4, 5, 6,dan 7 UU No 8 tahun 1999. Bahwa setiap pribadi berhak medapat perlakuan yang sama dalam hal untuk mengakses dan informasi. Artinya tiap *subscriber* bisa masuk ke dalam sistem ini jika memenuhi persyaratan, dan ia bisa mempergunakan sistem ini tanpa adanya hambatan. Dan *subscriber* juga berhak untuk didengar pendapat dan keluhannya.

## IV. Aspek Kritik Akademis tentang CA dalam UU ITE

### 4.1. CA Sebagai pondasi utama transaksi elektronik

CA merupakan lembaga yang mengatur berbagai regulasi kepercayaan di dalam transaksi elektronik, hal ini bisa di lihat pada uraian-uraian sebelumnya, dimana CA berwenang untuk :

1. Mengeluarkan (*issuer*) sertifikat digital
2. Mengatur penggunaan tanda tangan digital, distribusi kunci publik & pribadi (*public & private key*)
3. Sebagai lembaga yang mengeluarkan Trustmark (sertifikasi keandalan)

Sehingga pelaksanaan pasal-pasal transaksi elektronik dalam UU ITE seharusnya menunggu Peraturan Pemerintah yang mengatur regulasi CA sebagai pondasi utama transaksi elektronik

### 4.2. Haruskah CA berbadan hukum dan beroperasional di Indonesia

Seperti yang termaktub di dalam pasal 13 dalam UU ITE, CA atau penyelenggara sertifikasi elektronik Indonesia harus berbadan hukum Indonesia dan beroperasi di Indonesia. Namun yang terjadi dalam berbagai transaksi elektornik di Indonesia baik yang bernilai komersil (seperti transfer uang dalam internet banking BCA, Bank Mandiri & BII) maupun tidak, masih menggunakan CA Verisign yang berkedudukan di luar Indonesia.

Sehingga pasal 13 dalam UU ITE perlu di tinjau kembali agar dapat mengikat keluar dan ke dalam yuridiksi NKRI dan di sesuaikan dengan hukum internasional yang mengatur regulasi CA

### 4.3. CA Swasta atau pemerintah

Sertifikat keandalan seperti yang di atur dalam Pasal 10, merupakan kebutuhan pasar yang biasanya terbentuk dengan sendirinya atas permintaan pasar berupa lembaga non pemerintah (swasta). Sehingga jika CA yang di bentuk merupakan lembaga pemerinta maka netralitas CA terhadap badan-badan usaha milik pemerintah akan di pertanyakan oleh pasar

Jika pemerintah memang ingin membuat CA dalam waktu dekat, yang bisa mengakomodir keperluan transaksi elektornik, maka pemberdayaan YLKI (non pemerintah) dan Badan Perlindungan Konsumen Nasional (pemerintah) bisa di buat menjadi CA dengan mengikuti aturan-aturan internasional akan pembentukan CA

## V. Kesimpulan

1. Diperlukan hukum khusus yang bisa mengatur transaksi elektronis, bukan hanya melindungi produsen atau perusahaan tapi juga konsumen atau masyarakat umum pengguna internet sebagai media transaksi data.
2. Jelas semua transaksi yang bernilai komersil terjadi di internet yang melibatkan kedua belah pihak memerlukan pihak ke tiga (*Trusted third party*) atau CA sebagai jembatan

kepercayaan dan aspek legalitas kedua belah pihak yang bertransaksi, termasuk transaksi yang melibatkan pihak perbankan, atau institusi keuangan lainnya seperti jaringan pembayaran (Master Card; VISA dan lainnya).

3. Dalam kaitannya dengan penggunaan *digital signature* , CA dalam kedudukan yang lebih kuat harus bisa menjamin hak-hak konsumen. Terutama dalam perjanjian adhesi antara CA dan *subscriber.* Perjanjian diajukan sebaiknya tidak hanya berat sebelah, sehingga *subscriber* tidak mempunyai posisi penawaran (bargaining power).
4. Dalam UU ITE belum menjabarkan peraturan penyelenggara sertifikasi atau CA sehingga diperlukan peraturan lain sebagai persyaratan pelaksanaan pasal 12,13 dan 14 dalam UU ITE, namun di beberapa hukum nasional dan internasional dalam uraian sebelumnya pelaksanaan CA bisa dilakukan dengan mengambil persamaan materi muatan hukum.

**Daftar Pustaka**

Anonymous, *Undang-Undang No.11 Tahun 2008 Informasi dan Transaksi Elektronis*, Jakarta, 2008

Harris, Freddy., *Kesiapan Aspek Pengaturan Perundang undangan dalam Mengatasi Permasalahan Keamanan Transaksi Melalui Internet*
*(Keamanan Internet : Kebijakan Aspek Teknis dan Legal)*, Apricot, Bali, Febuari 2007

Mursito, Danan., Sirait, Raya Reinhardt., Wardhana, Sukma., *Pendekatan Hukum Untuk Keamanan Dunia Cyber Serta Urgensi Cyber law bagi Indonesia*, Jakarta, 2005

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

Ramli, Ahmad M., *Cyberlaw dan HAKI dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung, Oktober 2004

Wibowo, Arrianto Mukti., Makarim, Edmon., Yuristiawan, Hendra., Aulia, Muhammad., Sundoro, Erwin., Helena, Leny., Faraytody, Leo., Gaby, Patricia K., *Kerangka Hukum Digital signature Dalam Electronic Commerce*, Jakarta, Juni 1999