LAPORAN PENELITIAN TAHAP PERTAMA

Versi 1.04

NASKAH AKADEMIK RANCANGAN UNDANG UNDANG TENTANG TANDA TANGAN ELEKTRONIK DAN TRANSAKSI ELEKTRONIK

Prakarsa :

DIREKTORAT JENDERAL PERDAGANGAN DALAM NEGERI
DEPARTEMEN PERINDUSTRIAN DAN PERDAGANGAN
JAKARTA

Bekerja sama dengan :

LEMBAGA KAJIAN HUKUM TEKNOLOGI
FAKULTAS HUKUM UNIVERSITAS INDONESIA (LKHT-FHUI)
DEPOK

REPUBLIK INDONESIA 2001

KATA PENGANTAR

Penelitian ini dilakukan untuk merespons semakin pesatnya perkembangan Teknologi Informasi (IT) khususnya yang terkait dengan aplikasi perdagangan melalui media elektronik (elektronic commerce),yang berdasarkan pengalaman selain memberikan berbagai keunggulan serta menciptakan peluang usaha dan efisiensi,juga ternyata menimbulkan persoaalan-persoalanyang harus diantisipasi melalui kebijakan pemerintah.

Berdasarkan hal tersebut diatas,maka Departemen Perindustrian dan Perdagangan Cq.Direktorat Jenderal Perdagangan Dalam Negeri yang juga ditunjuk sebagai Kelompok Kerja Bidang Peraturan Per Undang-undangan dalam Tim Koordinasi Telematika Indonesia, setelah memperhatikan berbagai masukan dari Pelaku Usaha, Asosiasi, Perguruan Tinggi, Instansi Terkait dan masyarakat pada umumnya,maka pada tahun 2000 memprakarsai penyusunan naskah akademis Electronic Transaction and Electronic Transaction (ETES).

Diharapkan naskah akademis inidapat menjadi masukan dalam pembahasan yang lebih mendalam secara lintas sektoral untuk penyusunan landasan hukum yang memfasilitasi perkembangan electronic commerce di Indonesia.

Kepada Lembaga Kajian Hukum Teknologi (LKHT) Fakultas Hukum Universitas Indonesia disampaikan terima kasih atas kerja keras yang telah dilakukan sampai selesainya penyusunan laporan penelitian Electronic Transaction and Electronic Transaction (ETES) ini.

Semoga hasil penelitian ini dapat bermanfaat bagi perkembangan aplikasi electronic commerce di Indonesia.

DIREKTUR JENDERAL
PERDAGANGAN DALAM NEGERI

TEDDY SETIADY

RINGKASAN INFORMASI PENELITIAN

1	Judul	:	"Naskah Akademik Kerangka Hukum Indonesia Untuk Tanda Tangan Elektronik dan Transaksi Elektronik".
2	Bidang penelitian	:	Hukum, Teknologi Informasi
3	Penanggung jawab	:	Freddy Harris, SH, LL.M
4	Peneliti utama	:	Arrianto Mukti Wibowo, S.Kom
5	Peneliti	:	M. Aulia Adnan,SH Hendra Juristiawan, SH Rapin Mudiarjo, SH Wicaksono Wahyu Santoso, SH Parulian Aritonang Inderatna S. Depari Deddy Nurhidayat Fully Ridwan Riyanto R.
6	Rentan waktu	:	Agustus 2000 – April 2001 (penelitian awal/ fase pertama)
7	Institusi	:	Lembaga Kajian Hukum teknologi,Fakultas Hukum Universitas Indonesia.
8	Alamat	:	Gedung Fakultas Hukum , Lantai dasar University of Indonesia Depok, Jawa Barat, Indonesia 16424
9	Telepon	:	021-7863443/44#48, 7270003#48
10	E-mail	:	ikhtfhui@makara.cso.ui.ac.id (LKHT) amwibowo@cso.ui.ac.id,amwibowo@yahoo.com wicaksono@kompascyber.com,ulie@plasa.com
11	Fax	:	021-7270052
12	Situs internet	:	http://www.fh.iu.ac.id http://www.indocybeerlawnet http://www.hakinet.or.id

ABSTRAK

Laporan ini menjelaskan hasil-hasil yang dicapai dari fase pertama dari penelitian mengenai transaksi elektronik dan tanda tangan elektronik yang dilaksanakan oleh Lembaga Kajian Hukum teknologi Fakultas Hukum Universitas Indonesia (LKHT-FHUI). LKHT – FHUI adalah salah satu bagian dari kelompok kerja yang diinisiasikan oleh Departemen Perindustrian dan Perdagangan Republik Indonesia untuk melakukan kajian kebijakan dan peraturan mengenai e-commerce dan tanda tangan digital.

Fase pertama penelitian dilakukan dari bulan Agustus 2000 sampai bulan April 2001, dan memfokuskan diri untuk menentukan bagaimana transaksi elektronik dan tanda tangan elektronik dapat dimasukkan dalam kerangka hukum Indonesia yang sudah ada.

Ruang lingkup penelitian mencakup keberlakuan hukum transaksi elektronik dan tanda tangan elektronik dalam hukum Indonesia saat ini, kekuatan pembuktian tranaksi elektronik dan tanda tangan elektronik dalam persidangan, notarisasi dari transaksi elektronik dan tanda tangan elektronik, hak dan kewajiban dari pihak-pihak yang melakukan transaksi dalam suatu infrastruktur kunci publik (*public key infrastructure* atau PKI), standar untuk pengakuan terhadap transaksi elektronik dan tanda tangan elektronik, skim lisensi, dan masalah pengakuan standar antar negara.

Meskipun ada beberapa kemungkinan untuk menerima transaksi elektronik dan tanda tangan elektronik dalam kerangka hukum Indonesia yang berlaku saat ini, banyak yang membutuhkan interpretasi subyektif dari hakim. Masalah lain yang ada pada hukum yang berlaku sekarang adalah sedikitnya pengakuan secara eksplisit mengenai eksistensi transaksi elektronik dan tanda tangan elektronik, atau kalaupun ada pengakuan terhadap masalah itu, pengakuan itupun hanya berlaku untuk bidang tertentu saja.Karena itulah kami berpendapat bahwa hukum yang berlaku di Indonesia tidak memberikan solusi yang ”elegan” terhadap akseptansi hukum transaksi elektronik dan tanda tangan elektronik.Kami juga menyarankan agar perundangan mengenai transaksi elektronik dan tanda tangan elektronik segera dirancang untuk menjawab permasalahan-permasalahan diatas.

Kata kunci : hukum teknologi informasi,hukum transaksi elektronik,hukum tanda tangan digital

DAFTAR ISI

BAB 1
PENGANTAR

1.1 Latar belakang

Penelitian ini dimulai sebagai inisiatif dari Departemen Perindustrian dan Perdagangan pada bulan Mei 2000 untuk merancang kebijakan untuk bidang *electronic commerce*, terutama tanda tangan digital. Kelompok kerja untuk mempelajari maslaah ini dibentuk melalui keputusan Direktur Jenderal Perdagangan dalam Negeri nomor 14-1/DJPDN/VIII/2000.

Lembaga Kajian Hukum Teknologi, Fakultas Hukum Universitas Indonesia (LKHT-FHUI), merupakan bagian dari kelompok kerja yang dibentuk oleh Departemen Perindustrian dan Perdagangan tersebut, sebagai tim ahli. Oleh karena itu LKHT-FJUI melakukan investigasi lebih lanjut terhadap permaslahan hukum tanda tangan digital. Namun karena transaksi elektronikpun masih hanya diakui secara parsial dalam hukum Indonesia, maka kami memasukkan transaksi elektronik sebagai salah satu materi penelitian kami.

Oleh karena itu, penelitian ini diberi judul “Kerangka Hukum Indonesia Untuk Transaksi Eletronik dan Tanda Tangan Elektronik”.

1.2 Maksud Laporan

Laporan ini bertujuan untuk menjabarkan hasil-hasil yang dicapai selama penelitian tahap pertama “Kerangka Hukum Indonesia Untuk Transaksi Elektronik dan Tanda Tangan Elektronik” dilaksanakan dari bulan Agustus 2000 sampai Desember 2000.

Selain itu, laporan ini juga dipergunakan sebagai bahan pelengkap proposal guna mendapatkan dana penelitian tahap kedua.

1.3 Tujuan

Tujuan dari penelitian transaksi elektronik dan tanda tangan elektronik ini adalah :

1. Mencari kerangka hukum untuk transaksi elektronik dan tanda tangan elektronik berdasarkan hukum Indonesia yang berlaku saat sekarang.
   Hal ini disebabkan karena asas pengadilan Indonesia mengharuskan hakim untuk etap menerima suatu sengketa yang dibawa kehadapannya meskipun tidak ada hukum yang mengaturnya (pasal 22 *Algemeine van Bapelingen*), dan sang hakim diharuskan menggali hukum yang hidup di masyarakat (UU Pokok Kehakiman).

2. Membuat sebuah naskah akademik sebagai dasar pemikiran maupun kerangka untuk perancangan pengundangan transaksi elektronik dan tanda tangan elektronik.

3. Merancang draft akademik dari perundangan transaksi elektronik dan tanda tangan elektronik sebagai rekomendasi terhadap pemerintah.

1.4 Hasil- hasil yang dicapai

Pada penelitian pertama (Agustus–Desember 2000), kami berhasil merampungkan point pertama dari penelitian transaksi elektronik dan tanda tangan elektronik ini. Laporan ini selain menjelaskan bagaimana transaksi elektronik dan tanda tangan elektronik dapat dilihat dari kerangka hukum yang berlaku di Indonesia saat ini, juga memberikan pengantar terhadap beberapa aspek lainnya seperti pengentar kriptografi kunci publik.

Tujuan kedua dan ketiga dari penelitian ini diharapkan dapat dicapai pada tahap kedua dari penelitian ini, yang direncanakan akan dilaksanakan pada bulan Maret sampai Oktober 2001.

1.5 Ruang Lingkup

Penelitian transaksi elektronik dan tanda tangan elektronik yang kami lakukan mencakup :

- transaksi elektronik secara umum, kontrak, kesepakatan dan pencatatan.
- tanda tangan elektronik (tanda tangan digital).
- proses litigasi / persidangan untuk trnasaksi elektronik dan tanda tangan elektronik, guna memberikan bobot pembuktian pada transaksi elektronik dan tanda tangan elektronik.
- Hak dan kewajiban pihak-pihak yang bertransaksi dalam infrastruktur kunci publik (publik key infrastructure atau disingkat PKI).
- Pengakuan standar transaksi elektronik dan tanda tangan elektronik dan kemungkinan skim lisensi.
- Pengakuan tanda tangan digital antar negara.
- Aspek asuransi dalam infrastuktur kunci publik (PKI).

Dalam laporan ini menjelaskan konsep-konsep dasaer kriptografi dan juga PKI.

1.6 Pelaksanaan penelitian dan metodologi

Dalam fase pertama dari penelitian, kami telah melakukan penelitian literatur dalam aspek teknis dari transaksi elektronik dan tanda tangan elektronik dan juga menelitibeberpa perundangan transaksi elektronik dan tanda tangan elektronikdari beberapa negara lain (banyak diantaranya merupakan digital signature law, meskipun juga ada yang berupa e-commerce law atau e-transaction law). Setiap peneliti diwajibkan untuk

memberikan presentasi kepada peneliti yang lain untuk memperluas wawasan. Bahkan sebenarnya, proses pembelajaran dalam penelitian ini memakan waktu sekitar dua bulan sebelum penelitian sesungguhnya dilakukan.Dengan menarik isu-isu dari literatur-literatur yang didapatkan (terutama dari perundangan negara-negara lain), dilakukan identifikasi terhadap masalah-masalah utama . Dari setiap maslah tersebut, problem digali dan diformulasikan secara lebih detail . Satu atau dua orang peneliti berkewajiban untuk meneliti minimal satu problem besar. Tujuan dari penelitian terhadapproblem tersebut pada dasarnya adalah penelitian hukum, dimana dalam kasus ini berusaha mencari kerangka hukum untuk problem–problem tersebut.

1.7 Struktur Laporan

Laporan dimulai dengan menjelaskan konsep dasar kriptografi dan konsep dasar dari infrastruktur kunci publik pada bab 2.

Bab 3 menjelaskan mengenai kerangka hukum untuk transaksi elektronik termasuk mengenai data messege, kontrak elektronik, pencatatan elektronik, pertukaran pesan dan tanda tangan elektronik.

Bab 4 menjelaskan bagaimana transaksi elektronik dapat memiliki kekuatan hukum dalam acara persidangan. Tujuannya adalah untuk membuka kemungkinan transaksi elektronik sebagai alat bukti yang kuat dipengadilan. Keberadaan bea materai juga dibahas dlaam bab ini.

Bab 5 menjelaskan mengenai status suatu catatan elektronik yang setara dengan akta otentik. Tujuannya adalah unutk dapat mengenali, catatan elektornik macam apa yang dapat disejajarkan kekuatan hukummnya dengan data otentik.

Bab 6 menjelaskan mengenai hak dan kewajiban pihak-pihak yang terdapat dalam sebuah infrastruktur kunci publik.

Bab 7 menjelaskan mengenai standar yang diterapkan untuk menakui keberadaan hukum dari tanda tangan elektroni, termasuk kemungkinan skim lisensi untuk otoritas sertifikasi atau penyedia jasa kriptografis.

Bab 8 menjelaskan mengenai bagaimana juridikasi suatu negara dapat mengakui tanda tangan elektronik yang dibuat di juridikasi nehara lain. Hal ini amat penting untuk kompatibilitas tanda tangan elektronik lintas batas.

1.8 Status Laporan

Secara formal, penelitian tahap satu ini selesai pada bulan April 2001 . Namun karena sebenarnya laporan ini harus bisa menjelaskan dengan baik konstruksi hukum Indonesia pra perundangan tentang trasaksi elektronik dan tanda tangan elektronik, maka perbaikan dilakukan terus sampai terbentuknya perundangan yang baru

Untuk mengetahui perubahan-perubahan yang telah dilakukan pada laporan ini sejak april 2001, pembaca dapat melihat lampiran 1 mengenai perbaikan versi laporan.

Versi terbaru dapat diminta peminat dari para penulis via e-mail.

1.9 Terminologi

Dalam laporan ini, kami mendefinisikan ‘ transaksi elektronik’ sebagai :

> *“segala macam data elektronik, informasi elektronik atau catatan elektronik yang mempengaruhi dua orang atau lebih dan memiliki implikasi hukum:.*

jadi ‘transaksi elekronik’ mencakup kontrak digital, dokumen dalam hard disk atau floppy disk, data-data transaksi keuangan, pesan-pesan EDI, dan sebagainya.

Kami mengambil defenisi ‘tanda tangan elektronik’ dari UNCITRAL Uniform Rules on Elektronic Signatures Draft versi Februari 1999 :

> *“data in electronic form in, affixed to,or logically associated with, a data message, and that may be used to identifi the signature*

holder in relation to the data message and indicate the signature holder's approval of the information contained in the data message".

Dalam dokumen versi terakhir (september 2000) dari UNCITRAL Uniform Rulers on Electronic Signature Draft kami tidak menemukan defenisi dari 'electronic signatures' sehingga kami terpaksa menggunakan dokumen versi Februari 1999.

Dalam pembahasan nanti, kami berasumsi bahwa tanda tangan elektronik yang dimaksud dalam laporan ini, adalah tanda tangan elektronik yang berbasis pada infrastruktur kunci publik . Kunci publik dari seorang subjek hukum, disertifikasi keotentikannya oleh lembaga yang disebut dengan otoritas sertifikas (certification authority atau CA) . sedangkan Adams dan Lloyd mendefinisikan infrastruktur kunci publik sebagai

'security infrastructure implemented *using public key cryptography concept and techniques'*

Kata otoritas setifikasi (CA) sebenarnya mengacu pada pihak yang menandatangani sertifikat digital. Namun dalam laporan ini, kecuali secara spesifik disebutkan lain, kami menggunakan definisi yang lebih luas dari CA, yakni :

' *pihak yang bertanggng jawab terhadap seluruh pengoperasian infrastruktur kunci publik dan pengelolaan sertifikat digital '*

Definisi-definisi yang baru dijelaskan di atas mungkin hanya berlaku dalam laporan ini karena ada kemungkinan pada fase-fase selanjutnya dari penelitian transaksi elektronik dan tanda tangan elektronik ini, defenisi-defenisi tersebut dapat berubah karena adanya defenisi yang lebih bagus.

Bahkan ada kemungkinan kami menggunakan istilah yang lebih baik untuk menjabarkan suatu konsep, terutama kalau ada banyak perdebatan isi isu tersebut . Sebagai contoh, dalam laporan ini kami mengambil asumsi

bahwa konsep dasar dari tanda tangan elektronik adalah sama dengan konsep dasar dari ‘ tanda tangan digital’ . Bisa nanti saat penulisan di naskah akademik akhir, direkomendasikan pengunaan istilah ‘ tanda tangan digital’ karena lebih representatif untuk berbagai kondisi.

Selain itu, untuk menghindari kesalahpahaman, ada beberapa terminologi yang meskipun diterangkan dan diterjemahkan, namun untuk merujuk pada konsep tersebut tetap dipergunakan istilah umum dalam bahasa inggrisnya. Sebagai contoh, otoritas sertifikasi atau *certification authority* akan dirujuk dalam laporan ini dengan istilah ‘CA’. Demikian pula dengan infrastruktur kunci publik atau *public key infrastructure* akan dirujuk dengan istilah ‘PKI’.

Bab 2

KONSEP INFRASTRUKTUR KUNCI PUBLIK (PUBLIC KEY INFRASTRUCTURE/ PKI)

2.1 Latar Belakang

Meskipun cikal bakal Internet sudah ada sejak akhir dekade 1960-an, penggunaan Internet oleh masyarakat umum baru dimulai pada awal dekade 1990-an. Tidak lama setelah munculnya browser Mosaic (yang menjadi cikal bakal Netscape Navigator dan Microsoft internet Explorer), para pengusaha mulai melakukan bisnis di Internet sekitar tahun 1994-an, yang populer dengan sebutan Electronic Commerce (meskipun lebih tepat disebut sebagai Internet Commerce).

Kalau kita menggunakan istilah ‘ commerce’ atau ‘ perniagaan ‘ dalam bahsa Indonesianya, maka aktifitasnya adalah relasi antar perusahaan, jadi meskipun juga berkaitan dengan masalah administrasi intern perusahaan, namun fokusnya relatif mengenai masalah ‘external’ perusahaan . Contoh bagian-bagian yang terkait langsung dengan ‘ commerce’ adalah bagian marketing, inventory, public relation dan sebagainya.

Umumnya suatu transaksi perniagaan sifatnya rahasia (untuk kepentingan – kepentingan tertentu , misalnya pada perpajakan sifatnya terbuka). Padahal internet pada awalnya dirancang untuk kehandalan saluran komunikasi jaringan komputer saat perang nuklir, bukan untuk keamanan dan kerahasiaan data. Seluruh data yang dipertukarkan diinternet dapat dibaca dan ‘dikutak katik’ pihak ketiga ditengah jalan. Bahkan mahasiswa tingkat 3 disebuah perguruan tinggi jurusan ilmu komputer atau informatika, kadang kala mendapat tugas dari mata kuliah jaringan Komputer untuk ‘merakit ‘kembali data-data yang disadap dari jaringan komputer. Perlu diketahui bahwa tugas mata kuliah ini sama sekali bukan ‘ hacking’ dalam pengertian negatif. Secara tidak langsung hal ini menunjukan bahwa memang internet sama sekali tidak aman.

Sebenarnya, pentingnya keamanan dan kerahasiaan transaksi perniagaan ini bukan saja dengan media internet, namun juga pada media komunikasi lainnya . Jika wireless network (jaringan komunikasi udara tanpa kabel) ingin digunakan untuk transaksi perdagangan, maka tentu harus dilakukan pengamanan komunikasi yang memadai. Lagipula sebaiknya setiap transaksi perdagangan perlu diamankan ? Artinya, dengan menggunakan jaringan privatpun, sebaiknya ada langkah – langkah pengamanan data (terutama jika tidak mempercayai keamanan penyedia jaringan privat itu)

Ada beberapa trnsaksi yang perlu diamankan, sebagai contoh : transaksi keuangan, e-mail, file transer, tanda tangan suatu kontrak dalam bentuk digital, informasi dari perusahaan untuk publik (sehingga tidak bisa diubah-ubah orang lain), dan transaksi bisnis lainnya.

Bab ini akan dimulai dengan penjelasan mengenai teknologi dasar yang dipergunakan dalam pengamanan data untuk e-commerce, yakni kriptografi dengan fokus pada *publik key cryptography* (kriptografi kunci publik). Kemudian pada bagian selanjutnya akan dibahas mengenai infrastruktur kunci publik (*public key infrastructure yang disingkat PKI*) beserta pengelolaan infrastruktur tersebut. Selanjutnya akan dibahas mengenai *certificate policy* dan *certificate practice framework*. Pada akhir kita akan membahas mengenai masalah-masalah yang ada maupun yang timbul seputar PKI

Untuk mendapatkan spesifikasi lengkap mengenai PKI, pembaca dapat merujuk pada dokumen-dokumen RCF yang diterbitkan oleh Internet Engineering Task Force[2]. Adapun dokumen-dokumen yang berkaitan tersebut mencakup :

- RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC 2501: Internet X.509 Public Key Infrastructure Management Protocols
- RFC 2511 : Internet X.509 Certificate Request Message Format.
- RFC 2527 : Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

[2] *http://www.ietf.org*

- RFC 2528 : Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm(KEA) Keys in Internet X.509 Public Key Infrastructure Certificates.
- RFC 2559: Internet X.509 Public Key Infrastructure Operational Protocols LDA Pv2.
- RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol -OCSP
- RFC 2585: Internet X.509 Public Key Infrastructure Operational Protocols FTP and HTTP
- RFC 2587: Internet X.509 Public Key Infrastructure LDAPv2 Schema
- RFC 3029: Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols
- RFC 3039: Internet X.509 Public Key Infrastructure Qualified Certificates Profile.

2.2 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. Isu-isu dalam kriptografi meliputi :

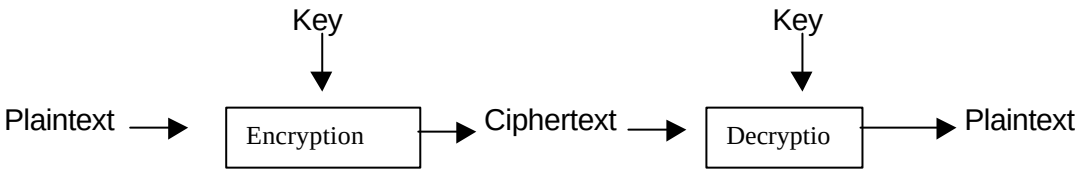
1. kerahasiaan (confidential) dari pesan dijammin dengan melakukan enkripsi (penyandian), sehingga pesan yang telah disandikan itu tidak dapat dibaca oleh orang-orang yang tidak berhak.
2. Keutuhan (integrity) dari pesan, sehingga saat pesan itu dikirimkan tidak ada yang bisa mengutak atik ditengah jalan. Sebagai contoh, dalam suatu transaksi pembayaran, sang pengirim pesan berkepentingan agar nilai cek digital sebesar Rp. 1.000.000,- tidak diubah orang lain menjadi Rp. 10.000.000,- ditengah jalan.
3. Jaminan atas identitas dan keabsahan (authenticity) jati diri dari pihak pihak yang melakukan trnsaksi. Sekedar ilustrasi, dari sisi konsumen, harus ada jaminan bahwa www.ibu-dibyo.co.id adalah benar benar ticket office milik ibu dibyo di Cikini. Sebaliknya, seorang pedagang di internet juga perlu mengetahui apakah seorang konsumen yang sedang

berbelanja di websitenya benar-benar menggunakan kartu kredit miliknya sendiri.

4. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (non repudiation) jika terjadi sengketa atau perselisihan pada transaksi elektronik yang telah terjadi.

Dalam kriptografi, ada dua proses utama :

1. Enkripsi (encryption) : yakni proses untuk mengubah pesan asli (plaintext) menjadi pesan yang tersandikan atau pesan yang terrahasiakan (ciphertext)
2. Dekripsi (decryption) : yakni proses mengubah pesan yang tersandikan (ciphertext) kembali menjadi pesan pada bentuk aslinya (plaintext).



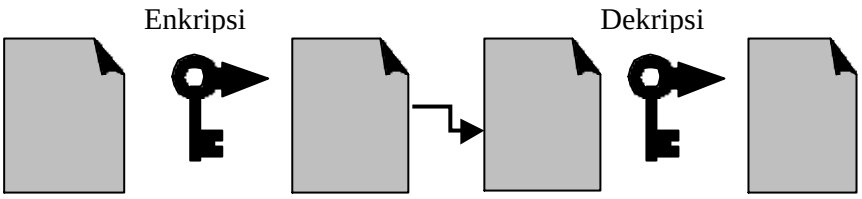
Gambar 1. Proses enkripsi dan dekripsi

Seperti akan kita lihat nanti, proses enkripsi dan dekripsi mengunakan kunci (key) 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.

2.2.1 Kriptografi Kunci Simetrik

Ini adalah jenis kriptografi yang paling umum dipergunakan. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu.Jadi pengirim pesan dan penerima pesan harus memiliki kunci yang sama persis . Siapapun yang memiliki kunci tersebut termasuk pihak-pihak yang tidak diinginkan dapat membuat dan membongkar rahasia ciphertext . Problem yang paling jelas disini terkadang bukanlan masalah

pengiriman ciphertextnya ,melainkan *masalah bagaimana meyampaikan kunci simetris rahasia tersebut kepada pihak yang diinginkan*. Dengan kata lain ada masalah *pendistribusian kunci rahasia* . Contoh algoritma kunci simetris yang terkenal adalah DES (data encryption standart) TripleDES, IDEA, Blowfish, Twofish, AES (advanced encryption standard) dan RC-4



Gambar 2. Penggunaan kunci simetris

2.2.2 Kriptografi kunci publik / kunci asimetrik

Teknik kriptografi kunci publik mencoba menjawab permasalahan pendistribusian kunci pada teknologi kriptografi kunci simetrik. Dalam kriptografi kunci publik, setiap pihak memiliki sepasang kunci :

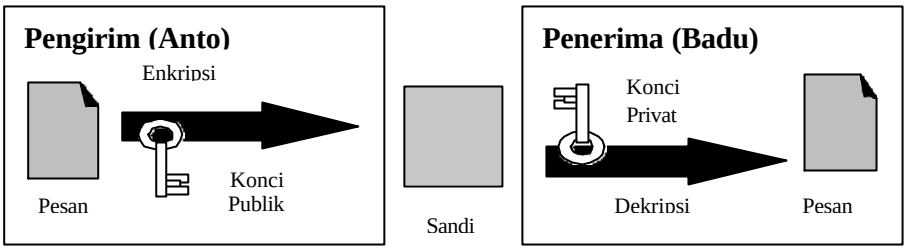
1. sebuah kunci publik yang didistribusikan kepada umum/ khalayak ramai.
2. Sebuah kunci privat yang harus disimpan dengan rahasia dan tidak boleh diketahui orang lain.

Dalam ilustrasi yang akan dijabarkan nanti, guna mempermudah penjelsan kita akan menggunakan beberapa nama ganti orang yakni Anto, Badu, Chandra dan Deni untuk mempresentasikan pihak-pihak yang melakukan transaksi.

Ada dua kegunaan mendasar dari setiap pasangan kunci – privat :

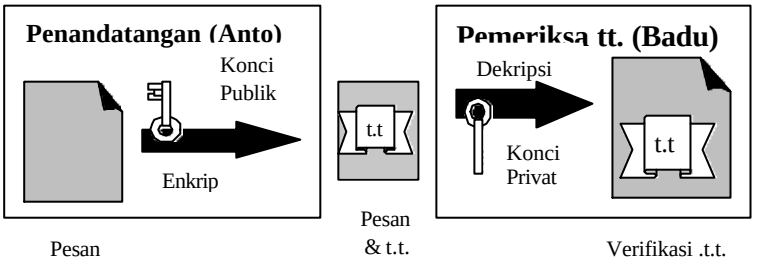
1. membungkus pesan sehingga kerahasiaannya terjamin . Siapapun Anto, Chandra dan Deni dapat mengirim pesan rahasia kepada Badu dengan cara mengenkripsi pesan asli (plaintext) dengan kunci publik milik Badu. Karena yang memiliki pasangan kunci

privatnya hanyalah Badu, maka tentu yang bisa membuka pesan rahasia hanyalah Badu.



Gambar 3. Pengiriman pesan rahasia (disederhanakan)

2. Menandatangani pesan untuk menjaga keotentikan pesan. Jika Anto hendak menandatangani suatu pesan , maka Anto akan menggunakan kunci privatnya untuk membuat tanda tangan digital. Semua orang lainnya (Badu, Chandra , Deni) bisa memeriksa tanda tangan itu jika memiliki kunci publik Anto.



Gambar 4. Penandatanganan pesan dan pemeriksaanya (disederhanakan)

Patut diperhatikan bahwa penggunaan kunci publik yang dijabarkan diatas merupakan penyederhanaan, sehingga tanda tangan digital akan dijelaskan secara lengkap dalam sub-bab tersendiri. Proses penyandian dan penandatanganan yang dipraktekkan, selain menggunakan teknologi kunci publik, juga memanfaatkan kunci simetrik dan fungsi hash.

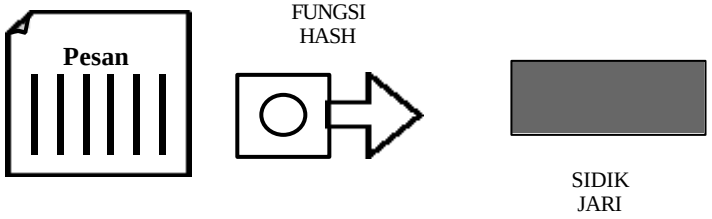
Contoh algoritma kunci publik yang sring dipakai adalah RSA, DSS (digital signature standard), El- Gamal, schnoor, Diffie –Hellman, dan ECC (Cleptic Curve Cryptosystem)

2.2.3 Fungsi Hash Satu Arah

Fungsi *hash* berguna untuk menjaga keutuhan (integrity) dari pesan yang dikirimkan.Bagaimana jika Anto mengirimkan surat pembayaran kepada Badu sebesar 1 juta rupiah, namun ditengah jalan Maman (yang ternyata berhasil membobol sandi entah dengan cara apa) membubuhkan angka 0 lagi dibelakangnya sehingga menjadi 10 juta rupiah ? Dimata Tari,pesan tersebut harus utuh, tidak diubah-ubah oleh siapapun, bahkan bukan hanya oleh Maman , namun juga termasuk oleh Anto,Badu dan gangguan pada transmisi pesan (*noise*). Hal ini dapat dilakukan dengan fungsi hash satu arah (*one way hash function*), yang terkadang disebut sidik jari (*fingerprint*), *hash, message integrity check* , atau *manipulation detection code*

.

Saat Anto hendak mengirimkan pesannya, dia harus membuat sidik jari dari pesan yang akan dikirim untuk Badu. Pesan (yang besarnya dapat bervariasi) yang akan di hash disebut pre-image, sedangkan outputnya yang memiliki ukurannya tetap, disebut hash value (nilai hush) . Kemudian , melalui saluran komunikasi yang aman, dia mengirimkan sidik jarinya kepada Badu. Setelah Badu menerima pesan si Anto – tidak peduli lewat saluran komunikasi yang mana – Badu kemudian juga membuat sidik jari dari pesan yang telah diterimanya dari Anto. Kemudian Badu membandingkan sidik jari yang dibuatnya dengan sidik jari yang diterimanya dari Anto. Jika kedua sidik jari itu identik, maka Badu dapat yakin bahwa pesan itu tidak diubah-ubah sejak dibuatkan sidik jari yang diterima dari Badu. Jika pesan pembayaran 1 juta rupiah itu diubah menjadi 10 juta rupiah, tentunya akan menghsilkan nilai *hash* yang berbeda.



Gambar 5. Membuat sidik jari pesan

Fungsi *hash* untuk membuat sidik jari tersebut dapat diketahui oleh siapapun, tak terkecuali, sehingga siapapun dapat memeriksa keutuhan dokumen atau pesan tertentu. Tak ada algoritma rahasia dan umumnya tak ada pula kunci rahasia.

Jaminan dari keamanan sidik jari berangkat dari kenyataan bahwa hampir tidak ada dua pre-image yang memiliki *hash value* yang sama. Inilah yang disebut dengan sifat *collision free* dari suatu fungsi *hash* yang baik.Selain itu , sangat sulit untuk membuat suatu pre-image jika hanya diketahui *hash* valuenya saja.

Contoh algoritma fungsi *hash* satu arah adalah MD-4, MD-5 dan SHA . *Message authentication code* (MAC) adalah satu variasi dari fungsi hash satu arah, hanya saja selain *pre-image*, sebuah kunci rahasia juga menjadi input bagi fungsi MAC.

2.2.4 Tanda Tangan digital

Badu memang dapat merasa yakin bahwa sidik jari yang datang bersama pesan yang diterimanya memang berkorelasi. Namun bagaimana Badu dapat merasa yakin bahwa pesan itu berasal dari Anto ? Bisa saja saat dikirimkan oleh Anto melalui saluran komunikasi yang tidak aman, pesan tersebut diambil oleh Maman. Maman kemudian mengganti isi pesan tadi, dan membuat lagi sidik jari dari pesan yang baru diubahnya itu. Lalu, Maman mengirimkan lagi pesan beserta sidik jarinya itu kepada Badu, seolah-olah dari Anto.

Untuk mencegah pemalsuan, Anto membubuhkan tanda tangannya pada pesan tersebut. Dalam dunia elektronik, Anto membubuhkan tanda tangan digital pada pesan yang akan dikirimkan untuk Badu sehingga Badu dapat merasa yakin bahwa pesan itu memang dikirim Anto.

Sifat yang diinginkan dari tanda tangan digital diantaranya adalah :

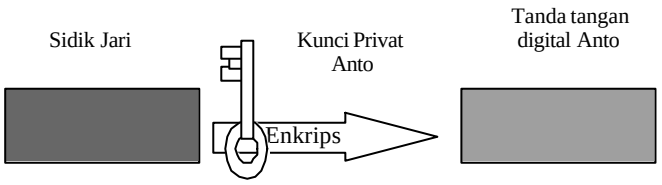
1. tanda tangan asli (otentik), tidak mudah ditulis/ ditiru oleh orang lain . Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang

bukti sehingga penandatangan tidak bisa menyangkal bahwa dulu ia tidak pernah menandatanganinya,

2. tanda tangan itu hanya sah untuk dokumen (pesan) itu saja . Tanda tangan itu tidak bisa dipindahkan dari suatu dokumen ke dokumen lainya . Ini juga berarti bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak sah lagi.
3. Tanda tangan itu dapat diperiksa dengan mudah.
4. Tanda tangan itu dapat diperiksa oleh pihak-pihak yang belum pernah bertemu dengan penandatangan.
5. Tanda tangan itu juga sah untuk kopi dari dokumen yang sama persis.

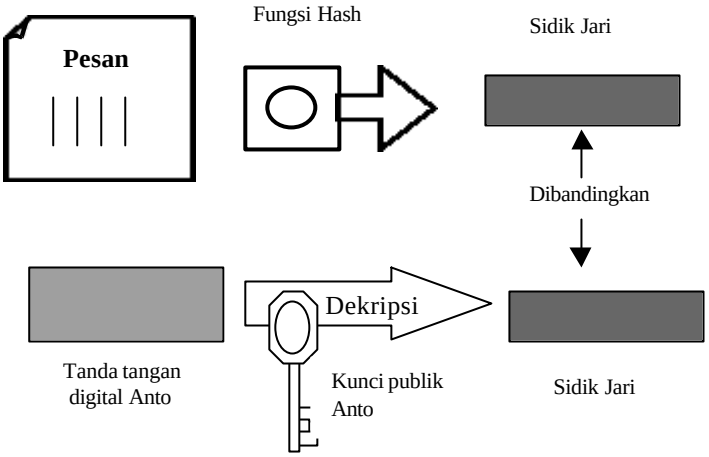
Meskipun ada banyak skenario, ada baiknya kita perhatikan salah satu skenario yang cukup umum dalam penggunaan tanda tangan digital . Tanda tangan digital memanfaatkan fungsi hash satu arah untuk menjamin bahwa tanda tangan itu hanya berlaku untuk dokumen yang bersangkutan saja.

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.



Gambar 6. Pembuatan tanda tangan digital

Keabsahan tanda tangan digital itu dapat diperiksa oleh Badu. Pertama-tama Badu membuat lagi sidik jari dari pesan yang diterimanya. Lalu Badu mendekripsi tanda atangan digital Anto untuk mendapatkan sidik jari yang asli. Badu lantas membandingkan kedua sidik jari tersebut. Jika kedua sidik jari tersebut sama, maka dapat diyakini bahwa pesan tersebut ditandatangani oleh Anto.



Gambar 7. Pemeriksaan keabsahan tanda tangan digital.

2.2.5 Sertifikat digital

Kriptografi kunci publik bukan tanpa masalah. Masalah utama adalah bagaimana orang-oranag bisa yakin bahwa kunci publik yang di 'duga' milik Badu adalah benar-benar milik Badu? Bukankah bisa saja Chandra membohongi Anto bahwa kunci publiknya adalah kunci publik milik Badu ?

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 ditanda tangani disebut dengan istilah sertifikat digital.Lembaga yang menandatangani sertifikat digital disebut dengan istilah *Certification Authority* (CA).Kita boleh membayangkan sertifikat digital berupa"tanda pengenal digital"

Keterangan yang ada dalam standar sertifikat digital X.509 versi 3 dan di RFC 2459 meliputi:

1.Versi sertifikat

2. Nomor seri sertifikat

3. Algoritma yang dipergunakan

4. Nama pemilik sertifikat digital,atau istilah lainnya adalah subject atau subscriber.Dilengkapi pula dengan keterangan mengenai pemilik,seperti :negara asal,organisasi,unit dalam organisasi itu,provinsi,dsb.
   Pada identitas"digital"dari pemilik sertifikat digital juga dicantumkan e-mail atau *domain name* websitenya (oleh karena itu untuk membuat sertifikat digital, sebuah perusahaan juga harus melampirkan surat keterangan yang menyatakan bahwa dirinya berhak menggunakan *domain name* tersebut)

5. Issuer,yakni lembaga yang menerbitkan sertifikat digital.

6. Validitas,yakni masa berlakunya sertifikat digital tersebut

.

7. *Extension* lainnya (sesuai kebutuhan penggunaan yang spesifik pada bidang tertentu) yang dapat meliputi:

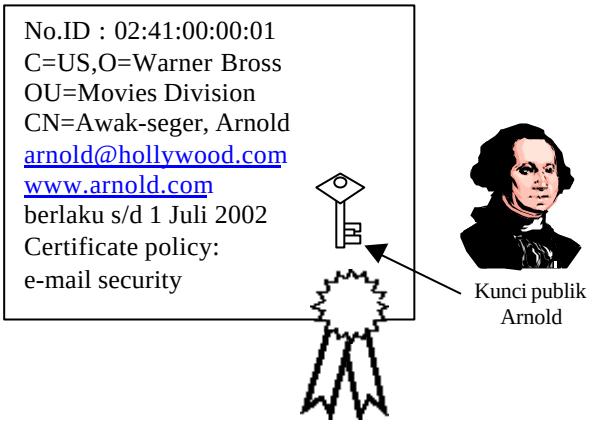
   - Nomor identifikasi kunci yang dipakai oleh CA (jika CA tersebut memiliki beberapa pasang kunci).
   - Nomor identifikasi kunci yang dipakai oleh subscriber (jika subscriber tersebut memiliki beberapa pasang kunci
   - Key Usage :menjelaskan bagaimana kunci itu dipergunakan secara teknis, apakah untuk penandatanganan,session key encryption,authenthication, dan sebagainya.
   - Extended key usage: menjelaskan untuk apa kunci itu di pergunakan: untuk server authentication(SSL/TLS), signing/authentication,time stamping.code signing,dan sebagainya.
   - CRL : lokasi dimana orang pemeriksa sertifikat dapat memeriksa lebih jauh, apakah sertifikat tersebut sudah dicoret/dibatalkan atau belum oleh issuernya.
   - Masa penggunaan kunci privat: menjelaskan sampai kapan kunci privat yang berpasangan dengan sertifikat digital ini masih berlaku.Hal ini disebabkan karena pendapat bahwa

sebaiknya masa berlaku kunci privat tidak perlu sama dengan masa berlaku kunci publik (meskipun masih diperdebatkan).

- *Certificate Policy* :berkaitan dengan bagaimana sertifiikat ini digunakan dalam kehidupan.Hal ini lebih berkaitan pada faktor manfaat bisnisnya. Contoh: ada sertifikat *certificate policynya* hanya boleh diperkenankan untuk mengamankan surat-surat biasa,sedangkan untuk mengamankan kontrak bernilai milyaran atau untuk mengamankan cek digital,maka diperlukan sertifikat jenis lainnya. Masalah certificate policy akan dijelaskan lebih terinci nanti.
- *Policy mapping:*jika dua (atau lebih CA) memiliki suatu kode *policy*yang berbeda untuk suatu jenis *policy* yang (kurang lebih)sama, maka kode tersebut dipetakan dalam CA.
- *Subject Alternative Name:*bisa berupa e-mail URI(Universal Resource Identifier),atau nomor Ipdari issuer.

- *Issuer Alternatvie Name:*bisa berupa e-mail, URI (U*niversal Resource Identifier)*atau nomor IP dari issuer.
- *Subject directory attbutes:*dipergunakan untuk atribut dari *Acces Control,*tetapi disarankan tidak untuk dipergunakan karena jika *attribut* itu diganti,maka terpaksa sertifikatnya di-*revoke.*
- *Basic constraint:*menjelaskan apakah sertifikat ini memiliki CA atau bukan.Jika merupakan sertifikat sebuah CA atau bukan.Jika merupakan sertifikat sebuah CA,maka juga ada field yang menjelaskan berapa banyak CA yang bisa ditelusuri dalam sebuah trust-network(certification path).
- *Name constraint:*menjelaskan CA mana saja yang diperkenankan atau dilarang ada dalam *certification path.*

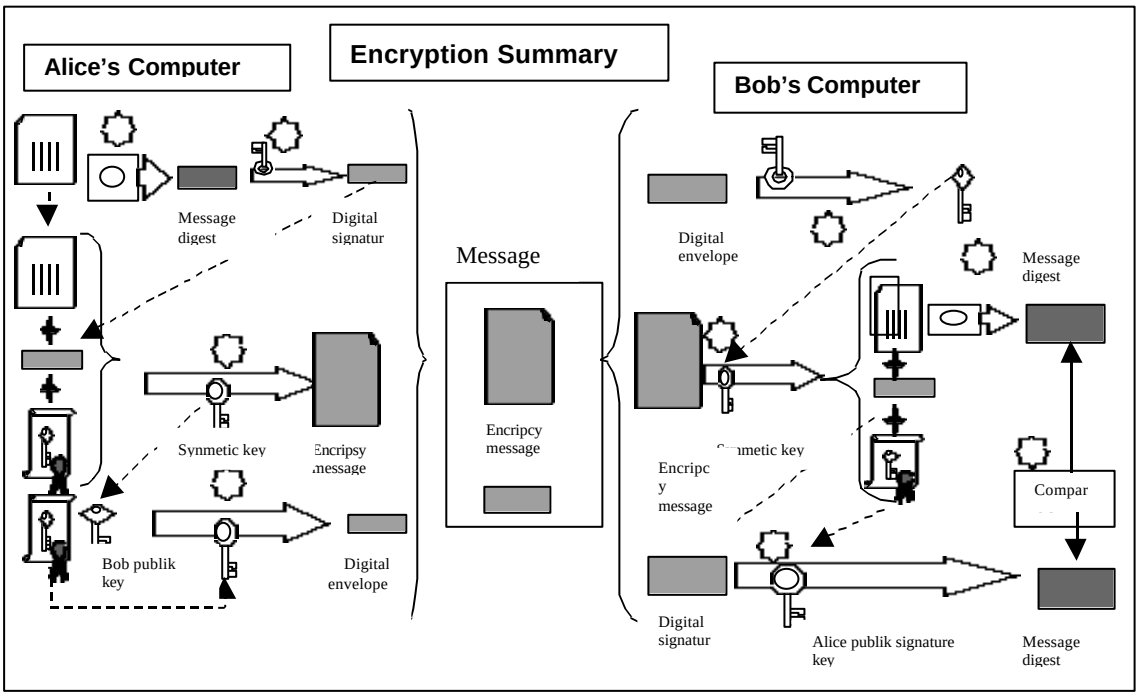
8. Tanda tangan CA pada sertifikat digital .



Gambar 8. Sertifikat digital

2.3 Transaksi Elektonik Dengan Kriptografi

2.3.1 Skenario transaksi elektonik dengan kriptografi kunci publik.



Gambar 9. Transaksi aman dengan PKI[3]

No	Penjelasan diagram
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 prifatnya sehingga ia akan mendapatkan digital signature dari data tersebut.
3.	Kemudian, Alice membuat (generates) suatu kunci simetris secara acak (random) dan mengunakan kunci itu melakukan enkripsi terhadap data yang hendak ia kirimkan , tandatangani (signature) miliknya, dan salinan dari sertifikat digitalnya yang berisi kunci publiknya . Untuk mendekripsi data tersebut Bob membutuhkan salinan dari kunci simetris tersebut.
4.	Alice harus memiliki terlebih dahulu sertifikat milik Bob, sertifikat ini berisi salinan (kopi) dari kunci publik milik Bob. Untuk menjamin keamanan transmisi dari kunci simetris maka kunci tersebut dienkripsi dengan menggunakan kunci publik milik Bob. Kunci yang telah dienkripsi yang dikenal sebagai amplop digital (digital envelope) akan dikirimkan bersama-sama dengan data yang telah dienkripsi.
5.	Alice kemudian akan mengirimkan data (message) tersebut yang berisi data yang telah dienkripsi dengan kunci simetris, tandatangan dan sertifikat digital, serta kunci simetris yang telah dienkripsi dengan kunci asimetris (digital envelope).
6.	Bob menerima pesan (message) dari Alice tersebut dan kemudian mendekripsi amplop digital dengan kunci prifat yang dipunyainya, ia kemudian akan mendapatkan kunci asimetris.
7.	Bob kemudian menggunakan kunci simetris tersebut untuk mendekripsi data itu (property descryption), tandatangan Alice dan sertifikat miliknya.
8.	Ia kemudian mendekripsi digital signature milik Alice dengan menggunakan kunci publik milik Alice, yang didapat Bob dari sertifikat milik Alice. Dari dekripsi ini akan didapatkan message digest dari data tersebut.
9.	Bob kemudian memproses (run) data itu dengan menggunakan algoritma satu arah yang sama yang digunakan Alice untuk message digest.
10.	Akhirnya Bob akan membandingkan antara message digest yang didapatkannya dari proses dekripsi diatas dengan message digest yang didapatkan dari digital signature milik Alice. Kalau hasil yang didapat dari perbandingan itu adalah sama, maka Bob dapat merasa yakin bahwa data tersebut tidak pernah dirusak (altered) selama proses transmisi dan data itu ditandatangani dengan mengunakan kunci privat milik Alice. Kalau hasil dari perbandingan itu adalah tidak sama maka data tersebut pastilah telah diubah atau dipalsukan setelah ditandatangani.

Tabel 1. Ringkasan mengenai cara komunikasi aman dengan kiptografi kunci publik.

[3] visa mastercard,secure electronic transmicion, book one, bussiness description,1997.http://www.setco.org

2.3.2 Panjang kunci dan keamanannya

Pembobolan kunci mungkin saja terjadi. Besar kecilnya kemungkinan ini ditentukan oleh panjangnya kunci. Semakin panjang kunci semakin sulit pula untuk membobolnya dengan *brute force attack.* Hal ini digambarkan dalam tabel berikut [4]:

	Panjang kunci (bit)					
ASIMETRIS (RSA)	-	384	512	768	1792	2304
Simetris (DES)	40	56	64	80	112	128
$ 100.000	2 detik	35 jam	1 thn	70000 thn	10^14 thn	10^19 thn
$1.000.000	0,2 detik	3.5 jam	37 hari	7000 thn	10^13 thn	10^18 thn
$ 10.000.000	0,02 detik	21 menit	4 hari	700 thn	10^12 thn	10^17 thn
$ 100.000.000	2 ms	2 menit	9 jam	70 thn	10^11 thn	10^16 thn

Tabel 2. Perkiraan waktu untuk membobol sebuah kunci dengan harga tertentu tahun 1995

Data tersebut merupakan perhitungan pada tahun 1995 dengan menggunakan hardware khusus untuk menjebol kunci simetris DES. Sedangkan kunci asimetris dalam kolom yang sama menunjukan panjang kunci asimetris yang memiliki kekuatan yang sama dengan kunci simetrisnya . Jadi untuk membobol kunci asimetris 512-bit membutuhkan waktu komputasi yang kurang lebih sama untuk membobol kunci simetris sepanjang 64 bit . Dengan asumsi kemampuan komputer menjadi berlipat ganda setiap 18 bulan dengan harga yang sama, maka pada tahun 1999 estimasi tersebut akan menjadi :

	Panjang kunci (bit)					
ASIMETRIS (RSA)	-	384	512	768	1792	2304
Simetris (DES)	40	56	64	80	112	128
$ 100.000	0.25 detik	44 jam	1.5 bulan	10000 thn	10^13 thn	10^18 thn
$1.000.000	25 ms	25 menit	4.5 hari	1000 thn	10^12 thn	10^17 thn
$ 10.000.000	2.5 ms	2.6 menit	12 jam	100 thn	10^11 thn	10^16 thn
$ 100.000.000	0.25 ms	2 menit	1.1 jam	10 thn	10^10 thn	10^15 thn

Tabel 3. Perkiraan waktu untuk membobol sebuah kunci dengan harga tertentu tahun 1999[5]

Berdasarkan data diatas terlihat bahwa resiko pembobolan kunci-kunci kriptografis, semakin tinggi sejalan dengan perjalanan waktu. Selain diperlukannya protokol-protool transaksi yang aman dari pencuri dan pembobolan, lembaga asuransi diharapkan dapat mengantisipasi kerugian yang mungkin terjadi dikemudian hari.

[4] *B.Schneier.Applied Cryptography:Protocols,Algoritms,and Sourece Code in C,2 edition (New York,John Wiley & Sons.Inc:1996)*

Titik rawan yang lain adalah munculnya teknologi komputer baru yang 'melanggar' moore's law, sehingga dengan teknologi komputer baru itu, kecepatan komputer meningkat berlipat-lipat secara signifikan. Akibatnya sertifikasi digital yang harusnya berlaku lebih lama, akan kadaluarsa lebih cepat karena dapat dibobol dengan mudah.

2.4 Public Key Infrastructure (PKI)

Public Key Infrastrukture (PKI) atau dalam bahasa Indonesianya infrastruktur kunci publik didefinisikan oleh Adams dan Lloyd sebagai :

> '*infrastruktur sekuriti yang diimplementasikan mengunakan konsep dan teknik kriptografi kunci publik*[6]

2.4.1 Entitas PKI

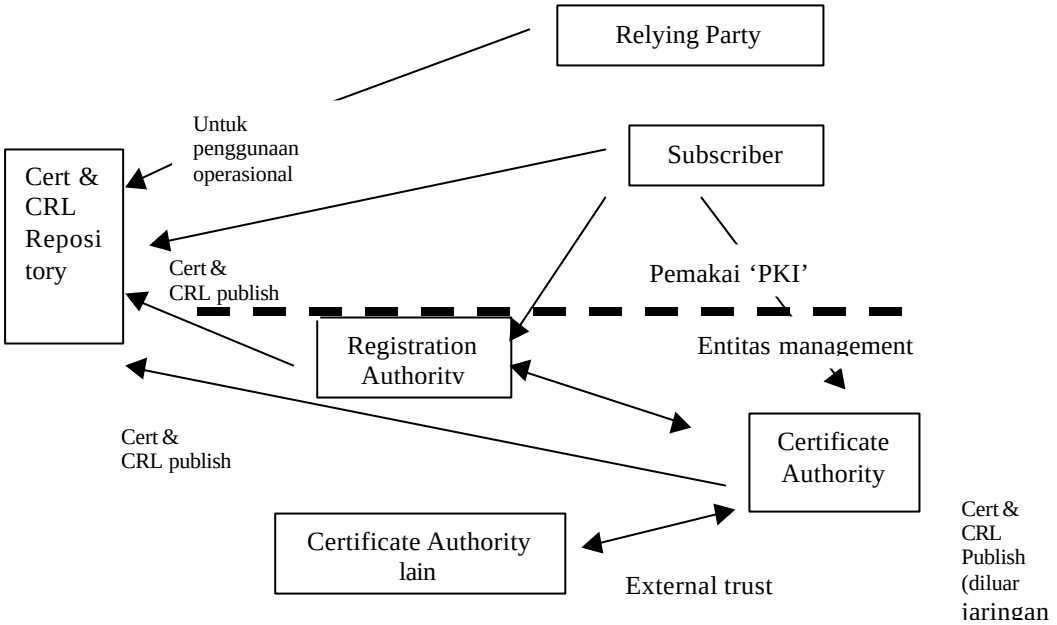
Menurut RFC 2510 tentang manajemen sertifikat , dalam sebuah model publik key infrastructure terdapat beberapa entitas :

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)

---

[5] *Wibowo,AM,Makarim, E,et.a.l, Kerangka Hukum Digital Signature Dalam Elektronic Commerce, (Depok, Fakultas Ilmu Komputer Univ Indonesia:1999), http://www.geocities.com/amwibowo/resource/hukum_ttd/hukum_ttd html*

[6] *C.Adams, and S Lloyd, Understanding Public key Infrastructure: Concepts, Standars, and Deplyment Concideration, (indianapolis, Macmillan Technical Publishing 2000)*



Gambar 10. Entitas dalam infrastruktur kunci publik

2.4.2 Subscriber

Pengertian dari seorang pelanggan *("subscriber"*) tidaklah mengacu hanya terbatas pada seorang subjek hukum saja. Sebenarnya subscriber dari sebuah sertifikat digital tidaklah harus orang atau perusahaan, namun bisa juga peralatan (*devide*) pada jaringan, aplikasi software dan *downloadable application.* Dalam RFC 2459, dipergunakan istilah '*subject*' untuk subscriber.

Seorang subscriber harus bisa menjaga private key-nya baik-baik, jangan sampai tercuri oleh orang lain. Ini amat penting, karena jika ada tanda tangan sang subcriber pada sebuah dokumen dapat diverifikasi dengan sertifikat digital yang bersangkutan, maka sang subscriber tidak bisa membantah bahwa dia telah menandatangani dokumen tersebut.

Untuk keamanan dari kunci privat *subscriber*, biasanya kunci itu disimpan dalam PSE (*personal security environment*) yang baik seperti dalam smartcard. Namun, karena faktor biaya, kadang kala kunci privat itu cukup dienkripsi (menggunakan PKCS#5) dalam sebuah file sehingga bisa diletakan di hard disk, disket atau CD-ROM.

2.4.3 Certification Authority

Certification Authority (CA) adalah sebuah lembaga yang bertugas mensertifikasi jati diri *subscriber / subject* agar *subscriber* itu bisa dikenali di dunia digital, dengan menerbitkan sertifikat digital untuk tiap *subscribernya.* Jika dianalogikan dengan penerbitan KTP di kelurahan, mungkin CA dapat disamakan posisinya dengan lurah yang menandatangani setiap KTP di kelurahannya. Hanya saja CA menandatangani 'KTP digital'. Tentunya CA harus merupakan entitas yang independen dan terpercaya (*trusted third party*) .

Untuk memberikan gambaran bagaimana CA bekerja kita ambil contoh bagaimana cara sebuah perusahaan meminta SSL. Perusahan itu perlu menunjukan kepada CA dua lembar surat, yakni surat ijin usaha dan surat izin penggunaan suatu *domain name* tertentu. Barulah setelah memeriksa keabsahan kedua dokumen tersebut, CA menrbitkan sertifikat digital SSL untuk perusahan yang bersangkutan.

Sebenarnya tidak harus pihak ketiga diluar organisasi sang *subscriber,* terutama untuk PKI yang tidak berhubungan dengan kepentingan publik. Misalnya , CA – internal disebuah perusahaan bisa saja mengeluarkan *digital ID* buat pegawainya , untuk keluar masuk ruangan (*accses control card)*

2.4.4 Registration Authority

Registration Authority (RA) bertanggung jawab untuk melakukan proses identifikasi dan otentikasi terhadap subscriber digital, tetapi tidak menandatangani sertifikat itu. Dalam kehidupan sehari-hari, banyak sekali dokumen yang diperiksa namun ditandatangani oleh orang yang berbeda.

Kembali ke contoh dikelurahan, saat kita mendaftarkan diri untuk membuat KTP baru, maka akta kelahiran, surat keluarga, dan surat keterangan RT akan diperiksa oleh pegawai tata usaha kelurahan. Nah, pegawai tata usaha kelurahan inilah yang dapat dianalogikan sebagai RA, karena yang menandatangani KTP tetap lurahnya (diibaratkan CA).

Adanya sebuah RA dalam PKI memang sifatnya *optional* (tidak harus ada) karena memang RA hanya menjalankan beberapa tugas yang didelegasikan oleh CA jika CA tidak sanggup melakukannya. Artinya, bisa saja dalam suatu skenario tertentu, seluruh tugas RA berada dalam CA. Menurut Adams dan Lloyd, tugas-tugas RA dapat mencakup[7] :

- Otentikasi calon subscriber secara fisik.
- Registrasi calon subscriber
- Membuat pasangan key untuk subsriber (jika subscriber tidak sanggup membuat sendiri pasangan kuncinya.
- Membuat backup dari kunci privat yang dipergunakan untuk enkripsi (key recovery)
- Pelaporan kalau ada sertifikat yang dicabut (revocation reporting)

2.4.5 Certificate Repository

Jika sebuah CA sudah menandatangani sebuah sertifikat digital, bukan berarti lantas seluruh permasalahan beres. Seorang subscriber, katakanlah Anto, bisa saja memegang sertifikat digital, dan Anto dapat menyerahkan sertifikat digitalnya kepada orang lain yang ingin berkomunikasi dengan aman dengan Anto. Teknik penyerahan sertifikat digital oleh pribadi ini disebut dengan istilah *private dessemination.* Tapi, teknik ini memiliki beberapa kekurangan :

1. Teknik ini hanya bisa untuk PKI dengan user dalam jumlah kecil. Artinya *scalability*-nya rendah, karena penyebaran informasinya tidak ‘meluas’.
2. Umumnya tidak sesuai dengan struktur perusahaan pada umumnya, yang cendrung sifatnya *centralized hierarchia*, ketimbang *user – centris*

[7] *Op.cit,Adams and Lloyd*.

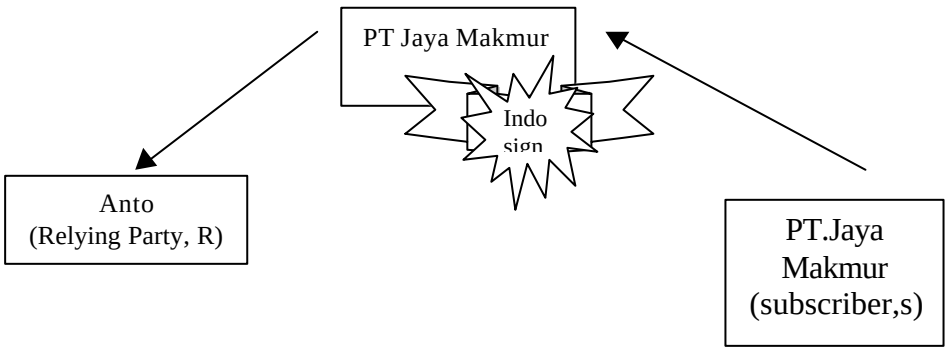
Namun dalam suatu skenario lain, Badu yang belum pernah berkomunikasi dengan Anto, hendak mengirimkan pesan rahasia kepada Anto. Nah, untuk itu, Badu perlu mendapatkan sertifikat digital Anto. Tetapi dari mana Badu mendapatkan sertifikat digital Anto?

Oleh karena itu, sebuah tempat penyimpanan (*repository*) on-line untuk sertifikat digital dibutuhkan dalam PKI. *Repository* ini juga berguna untuk menyimpan daftar sertifikat yang dibatalkan/CRL (yang tidak berlaku sebelum masa berlakunya habis). Jadi yang disimpan dalam repository bukan hanya sertifikat digital saja, namun informasi-informasi penting yang berkaitan dengan operasi sebuah PKI. *Repository* untuk sertifikat digital boleh diibaratkan seperti daftar alamat atau buku telepon.

Beberapa contoh yang masuk kategori *repository* mencakup : LDAP, X500, OCSP responder, database, dsb

2.4.6 Relying Party

Relying party adalah pihak yang mempercayai kebeadaan dan keabsahan suatu sertifikat digital. Dalam kasus pengiriman data rahasia (dengan amplop digital) dari Anto ke Badu, Anto mempercayai keberadaan sertifikat digital Badu. Dalam kasus ini, relying party-nya adalah Anto. Sedangkan dalam kasus penandatanganan surat oleh Anto, Badu memeriksa keabsahan tanda tangan Anto, adalah *relying-party*-nya.



Gambar 11. Konsep relying party

Untuk memberikan contoh lain, misalnya Anto mengakses sebuah secure website milik PT Jaya Makmur dengan SSL. Dalam koneksi SSL tersebut,

web server akan mengirimkan sertifikat digital milik PT Jaya Makmur, yang merupakan subscriber dari sebuah CA tertentu, Indosign[8] misalnya. Anto menggunakan sertifikat digital tersebut untuk melakukan proses otentikasi web server milik PT Jaya Makmur. Mungkin Anto mengenali dan mengakui keabsahan dari sertifikat digital tersebut karena :

1. Anto mengakui IndoSign sebagai pihak ketiga yang dipercaya yang melakukan proses sertifikasi. Karena itu, Anto mengakui keabsahan sertifikat yang ditandatangani IndoSign.
2. Sertifikat web server (SSL certificate) PT Jaya Makmur ditandatangani oleh IndoSign
3. Maka Anto mengakui keotentikan web server PT Jaya Makmur.

Dalam kasus ini, tergambar dengan jelas bahwa Anto adalah relying party.

2.4.7 Certificate Revocation List (CRL)

Meskipun sebuah sertifikat memiliki masa berlaku (sampai batas kadaluarsa) namun ada kalanya sertifikat tersebut harus dibatalkan keabsahannya atau dengan kata lain dicabut. Hal ini dapat terjadi kalau sang subscriber.

- tidak menjalankan kewajibannya sehingga sertifikatnya terpaksa dicabut.
- Mengganti namanya, atau ganti *address e –mail*, misalnya
- Kehilangan kunci privat pasangannya.
- Kunci privatnya berhasil dihack oleh orang lain

Daftar sertifikat yang dicabut sebelum kadaluarsa itu disebut dengan istilah *certificate revocation list*(CRL) dan disebarkan kepada publik melalui sebuah repository.CRL tersebut ditandatangani oleh CA,yang memuat :

1.Algoritma yang dipergunakan untuk menandatangani CRL

2.Nama pihak yang mengeluarkan CRL.

3.Tanggal/waktu saat CRL ybs dikeluarkan

4.Kapan CRL ybs akan kadaluarsa

[8] *Penyebutan nama CA dalam contoh ilustrasi dari hanyalah untuk memudahkan saja*

5.Kumpulan sertifikat yang dicabut :nomor seri, waktu pencabutan

6.Extension lainnya

Repository yang mengandung CRL yang di-*cache* di lokasi 'dekat'client,memungkinkan pengoperasian PKI secara off line,tanpa perlu terhubung dengan repository utama di CA sentral.Ini amat penting,karena berarti transaksi elektronik dapat berlangsung secara terdistribusi tanpa perlu adanya hubungan on-line ke pusat.

Namun kalau diperhatikan lebih jeli, maka ada jarak antara saat sertifikat dicabut,dengan waktu saat CRL diedarkan.
Nah,seharusnya, jika ada transaksi yang terjadi setelah tanggal pencabutan, maka transaksi tersebut harus dibatalkan.Namun jika transaksi tersebut ternyata tidak dapat dibatalkan,maka resiko harus ditanggung oleh perusahaan asuransi.

2.4.8.Online Certificate Status Protocol (OCSP)

Karena permasalahan data yang ada di CRL tidak realtime,maka mungkin untuk jenis aplikasi tertentu yang membutuhkan masalah besar. Misalnya , untuk transaksi fund-transfer bernilai tinggi, mungkin membutuhkan pengecekan validitas sertifikat secara real time.Dengan adanya Online Sertitificate Status Protocol (dispesifikasikan dalam RFC 2560) maka aplikasi-aplikasi yang menggunakan PKI dapat menentukan status keberlakuan dari sebuah sertifikat digital, apakah masih berlaku atau sudah dibatalkan. OCSP dapat dipergunakan untuk mendapatkan kejelasan status keberlakuan sebuah sertifikat digital dengan keakuratan yang jauh lebih baik ketimbang dengan CRL.Untuk melakukan pengecekan status sertifikat, sebuah client OCSP mengirimkan *status request* kepada OCSP responder. Client tidak akan mengakui keberadaan sertifikat yang bersangkutan,sebelum mendapatkan jawaban dari OCSP responder.

2.4.9. Key Backup & Recovery

Memang benar bahwa tujuan dari adanya kriptografi adalah memberikan proteksi kerahasiaan pada data. Dengan kritografi kunci publik, kerahasiaan terjamin karena kunci privat yang dipergunakan untuk proses

deskripsi ‘amplop’ digital, hanya diketahui oleh pemilik kunci privat yang sah.

Ada beberapa hal yang bisa memaksa kunci privat juga diback up oleh pihak ketiga yang dipercaya (trusted third party/ TTP), misalnya :

- kunci privatnya yang ada dalam harddisk, secara tidak sengaja sengaja terhapus,
- smart card yang dipergunakannya hilang atau rusak.
- ada pegawai kantor yang mengenskripsi data-data penting perusahaan menggunakan kunci publiknya, sehingga saat pegawai kantor berhenti bekerja,perusahaan tidak bisa membuka data-data penting tersebut.

Perlu dicatat,bahwa yang dibackup oleh TTP hanya *private descrition key* (kunci privat yang dipergunakan untuk mendeskripsi pesan),bukan *private signing key*,(kunci yang dipergunakan untuk membuat tanda tangan) . Hal ini disebabkan karena kalau yang di backup adalah pivate signing key,maka dikuatirkan terjadi pemalsuan tanda tangan. Dalam kasus dimana private signing key-nya hilang,maka terpaksalah sertifikat yang berkaitan dibatalkan(di-revoke),dan sebuah sertifikat digital baru diterbitkan oleh CA

.

2.4.10 Key Update/Certificate Renewal

Setiap sertifikat memiliki masa berlaku.tertentu.Saat mendekati masa kedaluarsa,sertifikat baru harus diterbitkan oleh CA untuk menggantikannya.Proses inilah yang disebut dengan *key update* atau pembaharuan sertifikat. Biasanya saat sertifikat berumur 80%.atau 70% dari masa berlakunya,sertifikat baru diterbitkan untuk menggantikan yang lama.Tujuan penggantian kunci ini (*key roll over*) adalah agar transaksi bisnis yang menggunakan PKI tidak terganggu kegiatan operasinya.

Key update juga berkaitan dengan masalah peningkatan keamanan kunci.Dalam sekuriti komputer, ada suatu kebiasaan agar selalu mengganti *password* (dalam hal ini kunci) guna meningkatkan keamanan.*Key update* dapat dilakukan secara manual atau otomatis.

2.4.11 Key History

Berkaitan dengan adanya *key update,*maka Anto dalam suatu saat dapat memiliki beberapa kunci sekaligus (miliknya),yakni sebuah kunci yang masih ‘berlaku’,dengan kunci-kunci lainnya yang sudah kadaluarsa atau sudah dibatalkan. Jika Anto ingin melakukan proses deskripsi data yang dia enkripsikan 5 tahun yang lalu, maka Anto perlu menggunakan kunci yang dipergunakan 5 tahun yang lalu untuk mengenkripsikan data tersebut.

2.4.12 Time Stamping

Dalam bisnis, waktu terjadinya kesepakatan, kontrak atau pembuatan surat amatlah penting. Oleh karena itu, diperlukan suatu mekanisme khusus untuk menyediakan ‘waktu’ yang terpercaya dalam infrastruktur kunci publik.Artinya,’waktu’ tersebut tidak didapatkan dari ‘clock’ setiap komputer, namun didapatkan dari satu sumber yang dipercaya.Penyedia jasa sumber ‘waktu’ yang dipercaya,juga termasuk kategori TTP.Waktu yang disediakan oleh *time stamp server* ,tidaklah harus tepat sekali, karena yang paling penting adalah waktu ‘relatif’ dari suatu kejadian lain.Misalnya suatu transaksi *purchase order* terjadi sebelum transaksi *payment.*

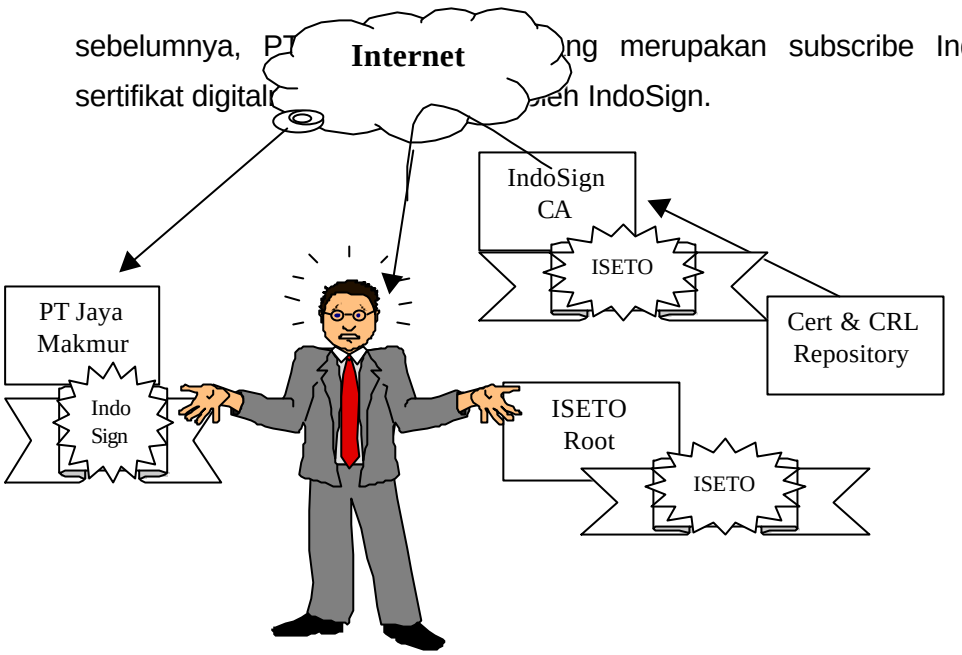
Meskipun demikian ,memang lebih bagus kalau waktu yang bersumber dari *time stamp server* mendekati waktu resmi (dari Badan Meteorologi dan Geofisika/BMG),misalnya.

2.5 Model-Model Jaringan Kepecayaan

2.5.1 Konsep Certification Path

Sebelum membahas lebih detail tentang *trust model*, maka perlu dibahas terlebih dahulu tentang *certification path.* Yang dimaksud dengan certification path adalah (penelusuran) rantai sertifikasi dari root CA ke subscriber, dimana di antara keduanya bisa ada beberapa CA lain. Sebagai contoh, ISETO (International Secure Electronic Transaction Organization, yang manajemen PKI –nya dipercayakan kepada WISEkey) adalah root CA global yang memiliki CA-CA lain sebagai anggotanya, seperti misalnya IndoSign. Artinya sertifikat digital IndoSign ditandatangani oleh ISETO. Pada gilirannya nanti, IndoSign akan melakukan sertifikasi terhadap perusahaan-perusahaan di Indonesia. Kembali kecontoh kita

sebelumnya, PT [illegible]ng merupakan subscribe IndoSign, sertifikat digital[illegible]eh IndoSign.



Gambar 12. Konsep penelusuran *certification path*

Andaikan ada seorang *relying party* dari Jepang, bernama Mitsuo yang hendak berdagang dengan PT. Jaya Makmur. Mitsuo hanya memiliki sertifikat digital ISETO saja. Saat Mitsuo mendapat sertifikat digital PT Jaya Makmur, maka sebenarnya Mitsuo tidak bisa 'mengakui' keberadaan sertifikat tersebut karena tidak mengenal 'siapa' IndoSign. Namun Mitsuo dapat menelusuri *certification path* dari sertifikat tersebut. Karena sertifikat PT. Jaya Makmur ditandatangani oleh IndoSign, maka Mitsuo akan berusaha mendapatkan sertifikat digital IndoSign dari repository. Mitsuo kemudian memeriksa keabsahan sertifikat digital IndoSign yang ditandatangani oleh ISETO dengan kunci publik dari sertifikat digital ISETO. Jadi, dalam kasus ini, certification path-nya adalah :

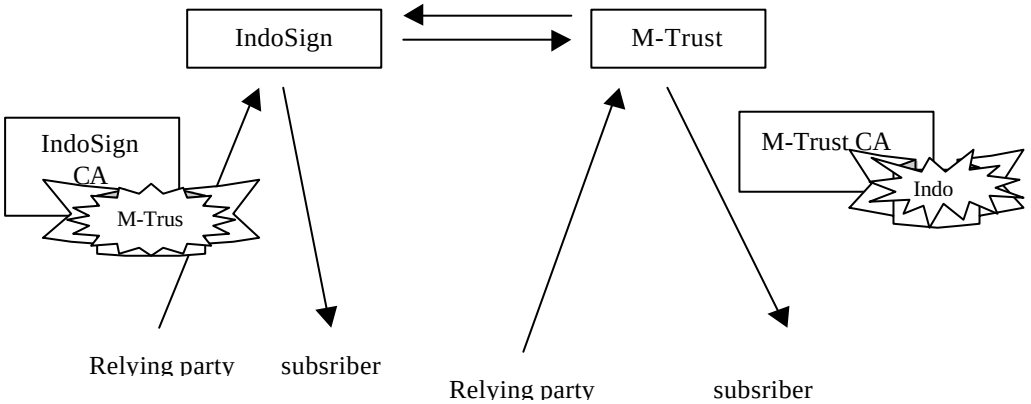
Sertifikat PT Jaya Makmur ⟶ Sertifikat Indo Sign ⟶ Sertifikat ISETO

Perhatikan bahwa sertifikat digital dari root CA selalu ditandatangani oleh dirinya sendiri (*self signed certificate*)

2.5.2 Cross- Certification

Di dunia cyber, seperti layaknya di dunia nyata sehari-hari, akan terdapat banyak pemegang kewenangan (otoritas) yang memberikan sertifikasi, surat izin, tanda pengenal, dan sebagainya.Lihatlah pada dompet anda, ada berapa kartu yang anda miliki? Artinya, pasti akan ada banyak CA didunia ini.

Namun tidak perlu dipungkiri, bahwa kebutuhan akan pengakuan keabsahan seorang subscriber dari *domain* CA yang lain, akan terjadi dalam suatu transaksi. Sebagai contoh, Anto yang merupakan seorang subscriber dari IndoSign (Anto berada dalam domain IndoSign), ingin berkirim e-mail dengan aman dengan Encik Badrul dari Malaysia, yang merupakan subscriber dari M-Trust (Encik Badrul berada dalam domain M-Trust) Jika antara M-Trust dengan IndoSign tidak ada hubungan apa-apa, maka Anto dan Encik Badrul tidak dapat berkomunikasi satu sama lain dengan aman. Hal ini disebabkan karena tidak ada 'trust' antar kedua domain yang berbeda itu.

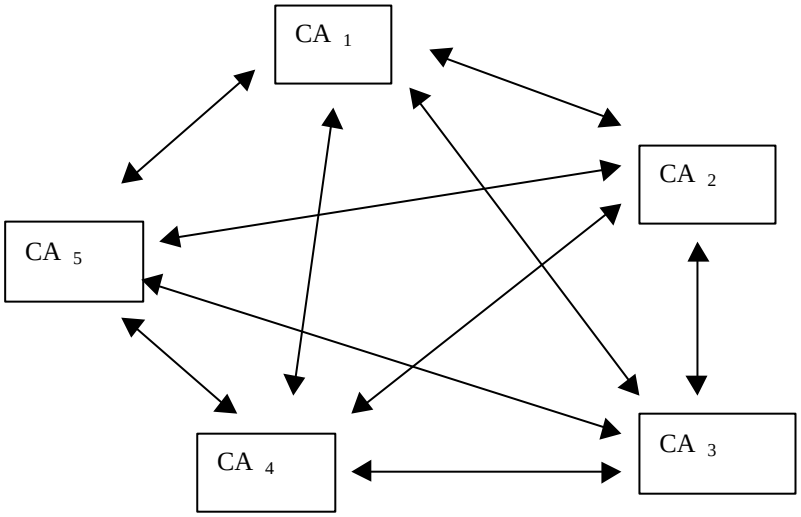


Gambar 13. Cross certification

Untuk membuat hubungan kepercayaan antara kedua domain tersebut, maka kedua CA tersebut saling menandatangani sertifikat yang lain. Selain sertifikat digital yang *self-signed*, setiap CA juga memiliki sertifikat digital yang ditandatangani CA dari domain yang lain. Teknik pengakuan antara

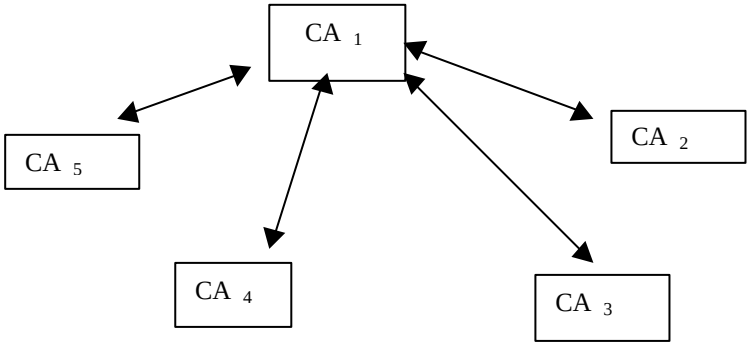
kedua CA dengan saling menandatangani sertifikat digital yang lainnya disebut dengan *cross certification* . Dengan adanya cross certification tersebut, Anto dapat mempercayai Encik Badrul dengan cara menelusuri certification path-nya.

Namun sayang, untuk banyak CA, teknik cross certification ini amat merepotkan. Jika dilakukan *full cross certification*, maka untuk 5 CA saja akan diperlukan 4+3+2+1 = 10 cross certification.



Gambar 14. Kerumitan cross certification

Sebenarnya kerumitan tersebut dapat disederhanakan dengan konsep *single hub cross-certification*. Dalam skenario ini ada sebuah CA yang dijadikan rujukan dimana CA-CA lain melakukan *cross certification* dengan CA rujukan.

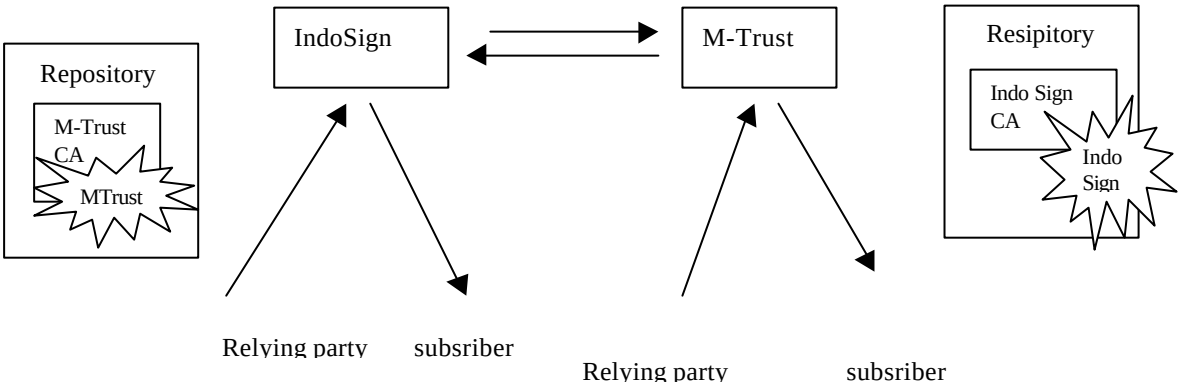


Gambar 15. Single hub cross certification

Artinya, *certification path* dari *subscriber -subscriber* yang ada dalam setiap *domain* ke *domain* yang lain, pasti melalui CA rujukan yang menjadi *hub*. Seperti akan kita lihat nanti, konsep ini memiliki kemiripan dengan trust model yang *hirarkis*

2.5.3 Cross-Registration

Ada cara lain untuk melakukan pengakuan antar domain CA, yakni dengan cara melakukan *cross –registration*. Dalam kasus ini, sebuah *domain* cukup menyimpan *root certificate* dari domain yang lain ke dalam *repository*-nya. Sehingga, jika seorang relying party sedang menelusuri *certification path* seorang *subscriber* dari domain CA yang lain, dia akan menemukan *root certificate domain* CA yang lain itu di *repository* lokal.

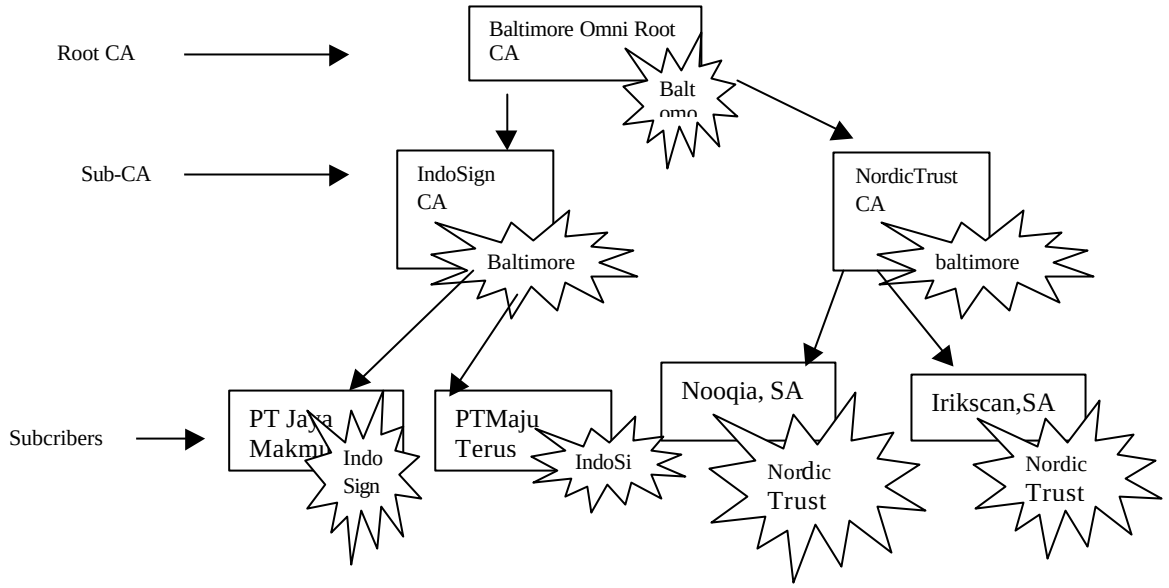


Gambar 16. Croos registration

2.5.4 Hirarkis

Cross certification biasanya dilakukan oleh CA-CA yang pada awalnya berdiri sendiri-sendiri, namun baru merasakan kebutuhan akan perlunya hubungan antar domain pada belakang hari.

Jika pada awalnya sudah dirasakan kebutuhan untuk hubungan antar domain maka sebuah sruktur baku yang hirarkis dapat menjadi model yang baik. Bahkan pada umumnya, model hubungan yang hirarkis diinisiasi / dimulai oleh sebuah root CA yang memiliki inisiatif untuk membangun sebuah *hierarchial trust tree.*



Gambat 17. Jaringan sertifikasi hirarkis

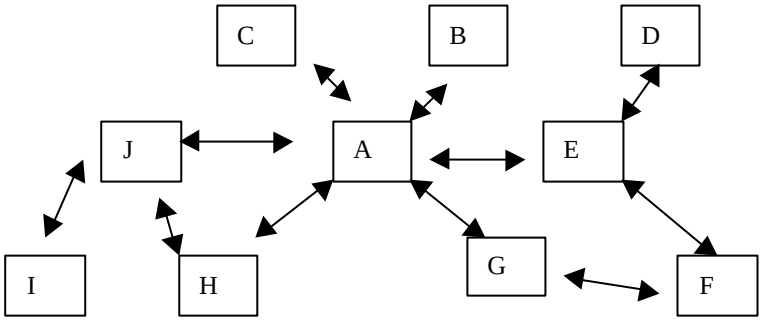
Sebuah root CA akan memiliki beberapa sub CA. Setiap sertifikat digital sub-CA ditandatangani oleh root CA. Namun, setiap *subscriber* dalam sub-CA, sertifikat digitalnya ditandatangani oleh sub-CA. Setiap *subsriber* yang berada dalam *tree*, hanya perlu memiliki root certificate saja untuk berkomunikasi dengan siapapun dalam *tree.*

Pola ini juga dianggap paling cocok dengan struktur perusahaan, sehingga pola ini banyak dipakai dalam bisnis.

Banyak trust network yang kita kenal menggunakan model hirarkis, seperti : ISETO / WISEkey, Identrus,Verisign, Baltimore OmniRoot (Cybertrust), dsb. Browser dan e-mail client seperti Microsoft Internet Explorer dan Netscape Navigator juga menggunakan varian dari pola hirarkis ini, hanya saja tidak menggunakan CRL. Pola jaringan kepercayaan hirarkis pada browser dan e-mail dikenal dengan istilah *web-model*.

2.5.5 User-centric web of Trust

Ada beberapa jenis trust network yang sangat terdistribusi, bahkan proses sertifikasi dari kunci publik tidak dilakukan oleh CA, melainkan oleh *end-entity*. Sebagai contoh dalam *web of trust* PGP (*pretty good privacy*), Joni (J) dapat berkomunikasi dengan Emir (E) karena jalur 'kepercayaan mereka' melalui Anto (A). secara teknis, jika A dan J saling mempercayai kunci publiknya satu sama lain, maka jika A menadatangani kunci publik E, maka J boleh jadi akan mempercayai E. Perhatikan bahwa tidak ada koordinasi sentral dari pola jenis ini.



Gambar 18. Pola Web of trust

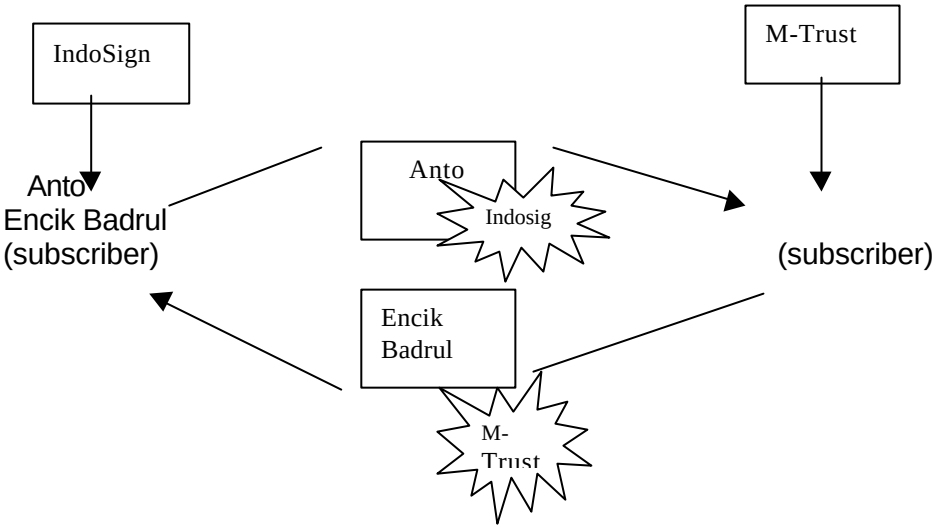
Pola ini berkembang di internet dengan dipelopori oleh Pretty Good privacy atau disingkat PGP yang dikembangkan oleh Philip Zimmerman [9]. Besarnya Web of Trust juga tidak menjamin bahwa Indra (I) dapat berkomunikasi dengan Dedy (D), karena certification pathnya sudah terlalu jauh. Artinya,semakin panjang certification path-nya, tingkat kepercayaannya juga semakin menurun. Selain itu, pola ini tidak cocok diterapkan dalam perusahaan –perusahaan yang pada umumnya memiliki stuktur hirarkis.

2.5.6 Direct End-Entity Trust

Dalam beberapa kasus, dapat saja terjadi Anto yang berada dalam domain yang berbeda dengan Encik Badrul, namun mereka berdua sudah

[9] *P.Zimmerman, The official PGP User's Guide (Cambridgr, MA, MIT Press:1995)*

mengenal satu sama lain dengan baik. Anto dan Encik Badrul saling mempercayai satu sama lain. Dalam kasus seperti ini, bisa saja terjadi *direct end entity trust*, dimana mereka saling mempertukarkan kunci publik (tepatnya, sertifikat digital) mereka masing-masing satu sama lain. Setelah itu, barulah mereka melakukan komunikaasi dengan aman. Karena domain tempat mereka tidak ada hubungan apa-apa, maka segala transaksi yang terjadi antara Anto dengan Encik Badrul, sepenuhnya bukan tanggung jawab CA manapun, melainkan pertanggungjawaban pribadi Anto dan Encik Badrul.



Gambar 19. Direct end-entity trust

2.6. Certificate Policy & Certificate Practice Statement

Tingkat kepercayaan seorang relying-party terhadap sebuah sertifikat digital tergantung pada beberapa faktor. Faktor-faktor tersebut termasuk :

- cara atau metodologi CA dalam mengotentikasi calon subscriber saat registrasi.
- Kebijakan CA, prosedure operasional CA dan manajemen keamanan yang diterapkan dalam CA.
- Kejelasan mengenai hak dan kewajiban subscriber
- Kejelasan mengenai hak dan kewajiban subscriber CA, termasuk tanggung jawab dan batas kerugian yang bisa ditanggung CA.
- dan sebagainya

2.6.1 Certificate Policy

Menurut standar RFC 2527, *certificate policy* adalah sekumpulan aturan yang menjelaskan bagaimana sebuah sertifikat itu diberlakukan pada suatu komunitas tertentu atau pada jenis transaksi / aplikasi tertentu, dengan suatu tingkat keamanan yang sederajat. Sebagai contoh, sebuah certificate policy bisa saja menunjukan bagaimana sertifikat digital bisa dipakai dalam transaksi EDI dengan suatu batas nilai transaksi tertentu. Dengan ada certificate policy, seorang relying party dapat menetukan apakah sebuah sertifikat (yang dapat mengikat sang *relying party*) cukup dapat dipercaya untuk dipakai mengamankan suatu jenis transaksi tertentu. Jadi bisa saja, seorang *relying party* tidak mempercayai sebuah sertifikat digital karena menurutnya mungkin sertifikat policynya tidak memenuhi syarat untuk pengamanan transaksinya.

Sertifikat digital X.509 versi 3, memiliki sebuah field yang menjelaskan certificate policy dari sertifikat yang bersangkutan. Sebuah sertifikat policy dipresentasikan dengan sebuah object identifier yang harus mengikuti prosedur standar dari ISO / IEC dan ITU. Artinya , 'teks' dari certificate policy tidak ada dalam sertifikat digital, melainkan ditunjuk oleh sebuah angka (object identifier). Ini adalah salah satu contoh dari incorporation by reference dari UNCITRAL *model law of e-commerce*.

Untuk memberikan sebuah gambaran mengenai *certificate policy*, kita ambil contoh mengenai IATA. Certification authority (CA)dari IATA akan membuat certificate policy untuk sertifikat-sertifikat digital yang diterbitkan dalam domain CA IATA. IATA bisa mendefinisikan 2 macam certificate policy :

1. *General purpose*

   Sebuah sertifikat digital yang memiliki policy ' general purpose", hanya bisa dipergunakan untuk keperluan rutin seperti e-mail, delivery order, cargo tracking, dan sebagainya. Batas ambang asuransinya juga tidal besar. Biasanya, cara mendapatkan sertifikat digital jenis ini cukup mudah, dimana seorang pegawai cukup mendaftarkan diri lewat web, dan mendapatkan sertifikat digital secara on-line. Bahkan, sang pegawai tidak perlu bertatap muka dengan RA. Syarat keamanan penyimpanan kunci privatnya pun rendah, cukup diletakan di disket saja.

2. *Commercial grade*

   Sedangkan sertifikat dengan policy “commercial grade” dipergunakan untuk transaksi-transaksi *high security* , seperti kontrak dengan supplier, fund-transfer antar bank, dan penjualan tiket pesawat on-line. Dalam kasus ini, mungkin subscriber harus menampilkan tanda pengenal didepan RA langsung sebelum menandatangani kontrak penggunaan sertifikat digital. Penyimpanan kunci privatnya pun mungkin diharuskan menggunakan smartcard. Tentunya batas ambang transaksi nya pun jauh lebih tinggi dan memiliki asuransi ganti rugi yang lebih baik juga.

2.6.2 Tingkat kepercayaan terhadap sertifikat

Tingkat keabsahan sertifikat digital sebenarnya tidak sama. Sebagai contoh, dalam Verisign Trust Network (VTN) ada beberapa kelas sertifikat. Cara mendapatkan sertifikat yang berbeda kelas, tidaklah sama. Disini juga berarti bahwa untuk setiap kelas, memiliki certificate policy yang berbeda-beda.

Ada sertifikat yang diberikan secara gratis. Sertifikat jenis ini (class 1) hanya bisa dipakai untuk menunjukan bahwa X adalah X. Namun ada juga sertifikat yang mahal sekali yang harganya mencapai ratusan dolar (misalnya *class 4 certificate*) Untuk mendapatkan sertifikat jenis ini, sebuah perusahaan harus menunjukan akta perusahaan, surat izin usaha dan surat izin penggunaan *domain name*. Secara fisik, harus hadir di CA untuk mendaftar.

Kesimpulan yang kita bisa tarik di sini adalah certificate policy atau level sertifikat menunjukan “trustworthiness” dari suatu subscriber.

2.6.3 Certification Practise Statement

Deskripsi yang lebih detail dari praktek operasional yang dilakukan oleh CA dalam registrasi calon subscriber, menerbitkan sertifikat, dan mencabut sertifikat (dengan kata lain memanage *life-cycle* sertifikat digital) tercantum dalam *Certification Practice Statement (CPS)* Menurut panduan tanda tangan digital dari American Bar Association (ABA), CPS adalah " *a statement of the practices which a certification authority employs in issuing certificates*." Penjelasan lengkap mengenai CPS dapat dilihat di dokumen RFC 2527.

Sebenarnya, CPS tidak hanya saja dapat berupa statement dari CA saja. Sebuah CPS juga bisa terdiri dari beberapa dokumen yang mencakup hukum publik, hukum privat dan pernyataan sepihak. Kepatuhan pada regulasi dari pemerintah mengenai syarat sebuah CA yang berlisensi juga dapat dijadikan salah satu bagian dari CPS. Kemudian, CPS juga bisa menjadi bagian dari kontrak antara CA dengan subscriber.

Kewajiban CA terhadap relying party juga dapat diletakan di dalam CPS. Meskipun relying party tidak terlibat 'kontrak' antara CA dengan subscriber namun relying party dapat melihat hak-haknya yang tercantum dalam CPS. Menurut RFC 2527, disarankan agar CPS dirujuk dari sertifikat digital (*incorporation by reference)* agar relying party dapat membaca CPS tersebut.

Berikut ini dalah contoh outline sebuah CPS yang direkomendasikan oleh RFC 2527 :

1. Intruduction
1.1 Overview
1.2 Indentification
1.3 Communicity and Applicability

    1.3.1 Certification authorities
    1.3.2 Registration authorities
    1.3.3 End entities
    1.3.4 Applicability

1.4 Contact Details

1.4.1 Specification administration organization

1.4.2 Contact person

1.4.3 Person determining CPS suitability for the policy

2. General Provision

2.1 Obligations

2.1.1 CA Obligations

2.1.2 RA obligations

2.1.3 Subscriber obligations

2.1.4 Relying party obligations

2.1.5 Repository obligations

2.2 Liability

2.2.1 CA liability

2.2.2 RA liability

2.3 Financial responsibility

2.3.1 Indemnification by relying parties

2.3.2 Fiduciary relationsips

2.3.3 Administrative processes

2.4 Interpretation and Enforcement

2.4.1 Governing law

2.4.2 Severability survival, merger, notice

2.4.3 Dispute resolution procedures

2.5 Fees

2.5.1 Certificate issuance or renewal fees

2.5.2 Certificate access fees

2.5.3 Revocation or status information access fees

2.5.4 Fees for other services such as policy information

2.5.5 Refund policy

2.6 Publication and repository

2.6.1 Publication of CA information

2.6.2 Frequency of publication

2.6.3 Access controls

2.6.4 Repositories

2.7 Compliance audit

2.7.1 Frequency of entity compliance audit

2.7.2 Identity/qualifications of auditor

2.7.3 Auditor's relationship to audited party

2.7.4 Topics covered by audit

2.7.5 Actions taken as a result of deficiency

2.7.6 Communication of results

2.8 Confidentiality

2.8.1 Types of information to be kept confidential

2.8.2 Types of information not considered confidental

2.8.3 Disclosure of certificate revocation/suspension information

2.8.4 Release to law enforcement officials

2.8.5 Release as part of civil discovery

2.8.6 Disclosure upon owner's request

2.8.7 Other information release circumstances

2.9 Intellectual Property Rights

3. Identifiction And Authentication (34)

3.1 Initial Registration

3.1.1 Types of names

3.1.2 Need for names to be meaningful

3.1.3 Rules for interpreting various name forms

3.1.4 Uniqueness of names

4.5.1 Types of event recorded
4.5.2 Frequency of processing log
4.5.3 Retention period for audit log
4.5.4 Protection of audit log
4.5.5 Audit log backup procedures
4.5.6 Audit collection system (internal vs external)
4.5.7 Notivication to event –causing subject
4.5.8 Vulnerability asseeements

4.6 Record Archival

4.6.1 Types of event recorded
4.6.2 Retention period for archive
4.6.3 Protection of archive
4.6.4 Archive backup procedures
4.6.5 Requirements for time-stamping of record
4.6.6 Archive collection to event –causing subject
4.6.7 Procedures to obtain and varify archive information

4.7 Key changeover
4.8 Compromise and Disaster Recovery
4.8.1 Computing resources, software, and/or external
4.8.2 Entity public key is revoked
4.8.3 Entity key is compromised

4.9 CA Termination

5. Physical, Prosedural, and Personnel Security Controls (34)
5.1.1 Site location and construction
5.1.2 Physical access
5.1.3 Power and air conditioning
5.1.4 Water exposures
5.1.5 Fire prevention and protection
5.1.6 Media storage
5.1.7 Waste disposal

5.1.8 Off-site backup

5.2 Procedural Controls

5.2.1 Trusted roles
5.2.2 Number of person required per task
5.2.3 Identification and authentication for each role

5.3 Personnel Controls
5.3.1 Background, qualifications, experience, and clearance requirement.
5.3.2 Background check prosedure
5.3.3 Training requirements
5.3.4 Retraining requirements
5.3.5 Job rotation frequency and sequence
5.3.6 Sanction for unautorized actions
5.3.7 Contracting personel requirements
5.3.8 Documentation supplied to personal

6. Technical Secutity Controls (34)
6.1 Key pair generation and installation

6.1.1 Key pair generation
6.1.2 Private delivery to entity
6.1.3 Public key delivery to certificate issuer
6.1.4 CA public key delivery to users
6.1.5 Key sizes
6.1.6 Public key parameters generation
6.1.7 Parameter quality checking
6.1.8 Hardware/ software key generation
6.1.9 Key usage purpose (as per x.509 v3 key usage field)

6.2 Private key protection

6.2.1 Standards for cryptographic module

6.2.2 Private key (n out of m) multi –person control

6.2.3 Private key escrow

6.2.4 Private key backup

6.2.5 Private key archival

6.2.6 Private key entry into cryptographic module

6.2.7 Method of activicating private key

6.2.8 Method of deacrivating private key

6.2.9 Method of destroying private key

6.3 Other aspect of key pair management

6.3.1 Public key archival

6.3.2 Usage periods for the public and private keys

6.4 Activation Data

6.4.1 Activation data generation and installation

6.4.2 Activation data protection

6.4.3 Other aspects of activation data

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

6.5.2 Computer security rating

6.6 Life Cycle Technical Controls

6.6.1 System development controls

6.6.2 Security management controls

6.6.3 Life cycle security ratings

6.7 Network security controls

6.8 Cryptographic module engineering controls

7. Certificate and CRL Profiles

7.1 Certificate profiles

7.1.1 Version number (s)

7.1.2 Certificate extennsions

7.1.3 Algorithm objec identifiers

7.1.4 Name forms

7.1.5 Name constraints

7.1.6 Certificate policy object identifier

7.1.7 Usage of policy constraints extension

7.1.8 Policy qualifiers syntax and semantics

7.1.9 Processing semantics for the critical certificate policy extension

7.2 CRL Profile

7.2.1 Version number (s)

7.2.2 CRL and CRL entry extensions

8. Specification Administration

8.1 Specification change procedures

8.2 Publication and notification policies

8.3 CPS appoval procedures

Bab 3

TRANSAKSI, PERJANJIAN DAN PERIKATAN

Pembahasan pada bab ini akan dimulai dari pembahasan mengenai konsep transaksi dan konsep perjanjian. Kemudian akan dilanjutkan pada konsep perikatan yang dihasilkan dari sebuah perjanjian.

Pembahasan kemudian dilanjutkan pada aspek transaksi elektronik, dimana kita-kita akan mengambil contoh pada transaksi EDI (termasuk di dalamnya EFT, elektronic fund transfers), dokumen elektronik yang ditandatangani secara digital, dan perjanjian berbasis web. Sebagian dari pembahasan transaksi elektronik akan mengacu pada UNCITRAL Model Law on e-commerce (revisi 1998)

3.1 Pengertian Transaksi

Transaksi yang berasal dari kata 'transaction', yang menurut The American Heritage Dictionary of English Language[10] memiliki makna :

1. *The act of transacting or the fact of being transacted.*
2. *Something transacted, especially a businnes agreement or exchange.*
3. *Communcation involving two or more people that affects all those involved*
4. *Transaction A record of business conducted at a meeting; proseding"*

Dalam laporan ini kami mengambil defenisi 'transaksi' yang kurang lebih mencakup butir 3 dan butir 4, dengan makna yang sedikit diperluas bahwa transaksi itu tidak hanya mencakup aspek bisnis saja. Alasannya adalah

[10] *The American heritage Dictionary of the English Language, Third Edition, 1996, Hougthon miffilin Company*

karena kita ingin agar defenisi transaksi ini juga mencakup hal-hal di luar hukum perdata.

Kata kunci yang perlu digaris bawahi dari butir 4 adalah ‘catatan’ (records) karena amat penting bagi pembuktian dimasa depan, namun tidak terbatas pada rapat-rapat (meeting) saja, melainkan dalam pengertian yang lebih luas. Perhatikan pula bahwa ‘catatan’ tersebut dapat disimpan dalam ingatan (otak). Jadi kalau diantara pihak-pihak yang bertransaksi tidak memiliki perbedaan persepsi yang prinsipil mengenai suatu transaksi, bisa saja transaksi tersebut tak tertulis di atas kertas. Kita akan lihat nanti bagaimana status suatu perjanjian (yang merupakan salah satu bentuk transaksi) lisan bisa mengikat.

Contoh dari suatu transaksi adalah berita, pernyataan, perintah, perjanjian dan sebagainya yang mempengaruhi orang lain. Perlu kami akui bahwa kami memang mengambil defenisi transaksi yang luas karena nanti akan berhubungan dengan defenisi ‘transaksi elektronik’.

3.2 Konsep Perjanjian

3.2.1 Pengertian Perjanjian

Perjanjian berasal dari kata ‘janji’ yang mempunyai arti “persetujuan antara dua pihak” (masing-masing menyatakan kesediaan dan kesanggupan untuk berbuat sesuatu). Defenisi ‘perjanjian’ seperti terdapat pada pasal 1313 KUHPerdata yaitu :

> *“Suatu perjanjian adalah suatu perbuatan dengan mana satu orang atau lebih mengikatkan dirinya terhadap satu orang lain atau lebih*”

sedangkan Prof Subekti memberikan pengertain perjanjian adalah sebagai berikut :

" suatu peristiwa di mana seorang berjanji kepada seorang lain atau dimana dua orang itu saling berjanji untuk melaksanakan sesuatu hal[11]"

Hal yang diperjanjikan untuk dilakukan itu dikenal dengan istilah 'prestasi'. Prestasi tersebut dapat berupa :

- memberikan sesuatu,
- berbuat sesuatu atau,
- tidak berbuat sesuatu.

Selain itu dalam hubungan antara penjual dan konsumen, hukum perjanjian berperan untuk memberikan suatu kepastian, stabilitas dan keamanan yang diperlukan untuk menjamin kelancaran dan pelaksanaan berbagai transaksi . Secara umum, hukum perjanjian mengatur hubungan pihak-pihak dalam perjanjian, akibat-akibat hukumnya , dan menetapkan bila pelaksanaan perjanjian dapat dituntut secara hukum.

3.2.2 Pengertian Perikatan

Menurut Prof Subekti SH, perikatan adalah

"suatu perhubungan hukum antara dua orang atau dua pihak, berdasarkan mana pihak yang satu berhak menuntut suatu hal dari pihak yang lain, dan pihak yang lain berkewajiban untuk memenuhi tuntutan itu"

Perikatan adalah suatu bentuk hubungan hukum, yang berarti bahwa hubungan tersebut diatur dan diakui oleh hukum. Segala sesuatu yang menjadi akibat atau konsekuensi dari timbulnya perikatan itu mendapatkan jaminan atas adanya kepastian hukum . Sebagai contoh, ketidakterlaksananya apa yang menjadi tuntutan atau dalam hal terjadinya wanprestasi terhadapt isi perjanjian, maka suatu transanksi hukum dapat dikenakan. Sanksi tersebut berupa pembayaran ganti kerugian oleh pihak yang melakukan wanprestasi atas kerugian yang diderita oleh pihak lawannya.

[11] *Subekti, Hukum Perjanjian, cet 16 (Jakarta:PT Intermasa, 1996) hal* 1

3.2.3 Perjanjian Satu Arah

Suatu perjanjian bisa dibuat secara timbal balik maupun yang hanya searah. Pada suatu perjanjian yang timbal balik dua orang pihak atau lebih saling memperjanjikan suatu hal yang akan menimbulkan hak dan kewajiban bagi kedua belah pihak. Perjanjian yang mempunyai sifat searah maka perjanjian ini hanya akan menimbulkan kewajiban bagi salah satu pihak saja. Contoh perjanjan yang bersifat searah adalah akta pengakuan hutang.

3.2.4 Hubungan Perjanjian Dengan Perikatan

Perjanjian yang terjadi diantara dua belah pihak mempunyai kekuatan mengikat bagi para pihak yang membuat perjanjian itu, seperti yang telah ditetapkan pada ketentuan pasal 1338 Kitab Undang-Undang Hukum Perdata. Munculnya kekuatan mengikat yang dari suatu perjanjian menunjukan adanya hubungan antara perikatan dan perjanjian, dimana perjanjian itu menimbulkan suatu perikatan. Jadi dapat kita katakan bahwa perjanjian adalah *sumber* perikatan.

Sebenarnya, perikatan juga bisa lahir dari Undang-Undang. Perbedaan diantara perikatan yang lahir dari perjanjian dengan perikatan yang lahir dari Undang-Undang adalah perikatan yang lahir dari perjanjian ini memang dikehendaki oleh kedua belah pihak sedangkan perikatan yang lahir dari undang-undang tidak berdasar atas inisiatif pihak-pihak yang bersangkutan.

Perlu diingat bahwa perikatan memiliki pengertian abstrak, maksudnya perikatan tersebut tidak dapat kita lihat secara langsung dengan mata kita atau dengan kata lain perikatan bersifat tidak kasat mata, perikatan hanya terdapat dalam bayangan atau dalam alam pikiran kita.

Sedangkan perjanjian itu dapat kita lihat wujudnya, diantaranya berupa suatu rangkaian perkataan yang mengandung janji-janji atau kesanggupan yang diucapkan atau ditulis, karena perjanjian merupakan suatu hal konkrit atau merupakan suatu peristiwa.

3.3 Asas asas Hukum Perjanjian

Buku III KUHPerdata mengenal tiga asas pokok dalam membuat dan melaksanakan suatu perjanjian. Ketiga asas tersebut adalah :

1. Asas kebebasan berkontrak atau sistem terbuka
2. Asas konsensualisme
3. Asas itikat baik

3.3.1 Asas kebebasan berkontrak atau sistem terbuka

Dikatakan bahwa hukum perjanjian menganut *sistem terbuka*, artinya hukum perjanjian memberikan kebebasan yang seluas luasnya kepada masyarakat untuk mengadakan perjanjian yang berisi apa saja, asalkan tidak melanggar aturan yang memaksa (*dwigned recht*), *ketertiban umum* dan *kesusilaan* . Para pihak diperkenankan untuk memperjanjikan hal-hal diluar undang-undang sesuai dengan kesepakatan bersama . Hal ini lebih dikenal dengan istilah 'hukum pelengkap'(*optional law / aanvulled recht)*, yang berarti bahwa pasal-pasal itu boleh disingkirkan manakala dikehendaki oleh pihak-pihak yang membuat perjanjian tesebut.

Mereka diperbolehkan mengatur sendiri kepentingan mereka dalam perjanjian-perjanjian yang mereka adakan itu. Kalau mereka tidak mengatur sendiri sesuatu permasalahan maka dalam hal permasalahan tersebut mereka tunduk pada ketentuan-ketentuan yang ada pada undang-undang. Hal dapat kita berikan contoh dalam perjanjian jual beli, cukuplah kiranya kita untuk setuju tentang barang dan harganya. Sedangkan tentang dimana barang harus diserahkan, siapa yang memikul biaya pengantaran barang, tentang bagaimana kalau barang itu musnah dalam perjalanan, soal-soal itu lazimnya tidak kita pikirkan dan tidak diperjanjikan. Cukuplah mengenai hal-hal tersebut kita tunduk saja pada hukum dan undang-undang.

Asas 'sistem terbuka ' dalam perjanjian,mengandung suatu prinsip kebebasan membuat perjanjian, dalam KUHPerdata lazimnya disimpulkan dalam pasal 1338 ayat (1) yang berbunyi demikian :

> *" semua perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya"*

Dengan menekankan pada perkataan ‘semua’ maka pasal tersebut seolah-olah berisikan suatu pernyataan kepada masyarakat bahwa kita diperbolehkan membuat perjanjian yang berupa dan berisi apa saja (atau tentang apa saja)dan perjanjian itu mengikat mereka yang membuatnya seperti suatu undang-undang. Dengan kata lain, hal membuat atau melakukan perjanjian, kita diperbolehkan memperjanjikan sesuatu bagi kita sendiri yang akan berlaku bagi para pihak dan mempunyai kekuatan hukum seperti halnya sebuah Undang-Undang [12]

3.3.2 Asas Konsensualisme

Dalam hukum perjanjian berlaku asas yang dinamakan asas konsensualisme. Perkataan ini berasal dari perkataan latin ‘consensus’ yang berarti sepakat. Asas konsensualisme ini bukanlah berarti suatu perjanjian disyaratkan adanya kesepakatan, tetapi hal ini merupakan suatu hal yang semestinya, karena suatu perjanjian juga dinamakan persetujuan, berarti dua pihak sudah setuju atau bersepakat mengenai sesuatu hal.

Arti asas konsensualisme ialah dasarnya perjanjian dan perikatan yang timbul karena nya itu sudah dilahirkan sejak detik tercapainya kesepakatan. Dengan perkataan lain, perjanjian sudah sah apabila sudah sepakat mengenai hal-hal pokok dan tidaklah diperlukan sesuatu formalitas tertentu,kecuali untuk perjanjian yang memang oleh Undang-Undang dipersyaratkan suatu formalitas tertentu.

Asas konsensualisme tersebut lazimnya disimpulkan dari pasal 1320 KUHPerdata ,yang berbunyi :

‘Untuk sahnya suatu perjanjian diperlukan empat syarat’ :

1. *sepakat mereka yang mengikat dirinya*
2. *kecakapan untuk membuat suatu perjanjian*
3. *suatu hal tertulis*
4. *suatu sebab yang halal*

[12] *Penting untuk diperhatikan didalam sebuah komunikasi elektronik,’sepakat’ adalah tergantung dari prosedur telekomunikasi yang akan dijalankan. Jika prosedur tersebut dipenuhi dan communication system itu berjalan sebagaimana mestinya, maka kesepakatan tersebut adalah sudah terjadi*

Oleh karena dalam pasal tersebut tidak disebutkan suatu formalitas tertentu di samping kesepakatan yang telah tercapai itu, maka disimpulkan bahwa setiap perjanjian itu sudah sah (dalam arti mempunyai kekuatan "mengikat" kepada para pihak yang membuatnya) apabila sudah tercapai kesepakatan mengenai hal hal yang pokok dari perjanjian tersebut.

Akan tetapi, terhadap asas konsensualisme ini, terdapat pengecualiannya . Di dalam Undang-Undang ditetapkan adanya formalitas-formalitas tertentu untuk beberapa macam perjanjian yang dapat berakibat pada batalnya perjanjian tersebut bila tidak mengikuti tata cara yang dimaksud. Sebagai contoh dalam perjanjian penghibahan, jika yang dihibahkan adalah benda tak bergerak, maka perjanjian harus dilakukan dengan akta notaris .Perjanjian – perjanjian untuk mana ditetapkan suatu formalitas tertentu dinamakan perjanjian formil

3.3.3 Asas Itikad Baik

Hukum perjanjian mengenal pula asas itikad baik seperti yang terdapat pada pasal 1338 ayat 3 KUHPerdata :

" *Suatu perjanjian harus dilaksanakan dengan itikat baik"*

Asas itikat baik ini menghendaki bahwa suatu perjanjian dilaksanakan secara jujur, yakni dengan mengindahkan norma-norma kepatuhan dan kesusilaan . Asas ini adalah salah satu sendi terpenting dari hukum perjanjian.

3.4 Syarat-syarat Sahnya Perjanjian

Berdasarkan ketentuan pasal 1320 KUHPerdata, untuk sahnya suatu perjanjian diperlukan syarat-syarat sebagai berikut :

1. *sepakat mereka yang mengikatkan dirinya.*
2. *Kecakapan untuk membuat suatu perikatan*
3. *Suatu hal tertentu*
4. *Suatu sebab yang halal*

Untuk dua syarat yang pertama, dinamakan syarat subjektif, karena kedua syarat tersebut mengenai orang-orangnya atau subjek-subjek hukum yang melakukan perjanjian. Sedangkan untuk dua syarat yang terakhir dinamakan syarat-syarat objektif karena keduanya berkaitan dengan perjanjiannya itu sendiri atau objek dari perbuatan hukum yang dilakukan itu.

Sepakat mereka yang mengikatkan dirinya, dimaksudkan bahwa para pihak yang mengadakan perjanjian itu harus bersepakat, setuju atau seia sekata mengenai hal-hal yang pokok dari perjanjian yang diadakan itu. Apa yang menjadi kehendak pihak yang satu, juga dikehendaki oleh pihak yang lain. Mereka menghendaki sesuatu yang sama secara timbal balik. Kecakapan untuk membuat suatu perikatan, hal ini mempunyai arti bahwa orang yang membuat suatu perjanjian harus cakap menurut hukum. Pada asasnya setiap orang yang sudah dewasa dan sehat pikirannya adalah cakap menurut hukum. Ketentuan mengenai kecakapan seseorang diatur dalam pasal 1329 sampai dengan pasal 1331 KUHPerdata.

Tentu saja bila dipandang dari sudut rasa keadilan, perlulah bahwa orang yang membuat suatu perjanjian yang pada akhirnya akan terikat oleh perjanjian itu, mempunyai cukup kemampuan untuk menyadari benar-benar akan tanggung jawab yang dipikulnya dengan perbuatannya itu.

Orang yang tidak sehat pikirannya tentu tidak mampu untuk menerima tanggung jawab yang dipikul oleh seorang yang mengadakan suatu perjanjian. Orang yang ditaruh di bawah pengampuan menurut hukum tidak dapat berbuat bebas dengan harta kekayaannya. Seseorang yang berada di bawah pengampuan kedudukannya sama dengan seorang anak yang belum dewasa. Kalau seorang belum dewasa harus diwakili oleh orang tua atau walinya maka seorang dewasa yang telah ditaruh dibawah pengampuan harus diwakili oleh pengampu atau kuratornya.

Suatu hal tertentu, sebagai syarat ketiga untuk sahnya suatu perjanjian. Suatu hal tertentu ini mengacu kepada apa (objek) yanng diperjanjikan dalam perjanjian tersebut. Barang atau objek tersebut paling sedikit harus ditentukan jenisnya . bahwa barang tersebut sudah ada atau sudah berada ditangannya si berutang pada waktu perjanjian dibuat, tidak diharuskan oleh undang-undang.

Suatu sebab yang halal, perlu untuk dijelaskan bahwa yang dimaksud dengan sebab disini tiada lain adalah isi dari perjanjian itu sendiri. Yang dimaksud kan dengan sebab atau causa dari suatu perjanjian adalah isi perjanjian itu sendiri sebagai ilustrasi : dalam suatu perjanjian jual beli isinya adalah pihak yang satu menghendaki uang dan pihak yang lain menginginkan hak milik atas barang tersebut. Dan sebab tersebut merupakan sebab yang halal yang mempunyai arti bahwa isi yang menjadi perjanjian tersebut tidak menyimpan dari ketentuan-ketentuan perundang-undangan yang berlaku di samping tidak menyimpang dari norma-norma ketertiban dan kesusilaan

3.5 Masa Berlakunya Perjanjian

3.5.1 Terjadinya Perjanjian

Menurut asas konsensualisme, suatu perjanjian lahir pada detik tercapainya kesepakatan atau persetujuan antara kedua belah pihak mengenai hal-hal yang pokok dari apa yang menjadi objek perjanjian. Sepakat adalah suatu persesuaian paham dan kehendak antara dua pihak tersebut. Apa yang dikehendaki oleh pihak yang satu, adalah juga dikehendaki oleh pihak yang lain, meskipun tidak searah tetapi secara timbal balik. Kedua kehendak tersebut akan bertemu satu sama lain.

Dengan demikian, untuk mengetahui saat lahirnya suatu perjanjian, harus dipastikan apakah telah tercapai kesepakatan antara para pihak yang berjanji. Haruslah dipegang teguh tentang adanya suatu persesuaian kehendak antara para pihak yang berjanji. Apabila kedua kehendak tersebut tidak saling bertemu atau saling berselisih, tak dapat dikatakan telah lahir suatu perjanjian. Karena suatu perjanjian lahir pada detik tercapainya kesepakatan, maka ada madzhab yang berpendapat bahwa perjanjian itu lahir pada detik diterimanya suatu penawaran (offerte). Artinya dengan diterimanya suatu penawaran maka dapat disimpulkan bahwa kedua belah pihak telah mengetahui tentang adanya penawaran tersebut. Dan pihak penerima penawaran melakukan penerimaan terhadap penawaran tersebut sehingga lahirlah suatu perjanjian.

3.5.2 Berakhirnya Perjanjian

Berdasarkan pasal 1381 KUHPerdata, perikatan-perikatan hapus (berakhir) :

- karena pembayaran;
- karena penawaran pembayaran tunai, diikuti dengan penyimpanan atau penitipan;
- karena pembaharuan utang
- karena perjumpaan utang atau kompensasi;
- karena percampuran utang;
- karena pembebasan utang;
- karena musnahnya barang yang terutang;
- karena kebatalan atau pembatalan;
- karena berlakunya suatu syarat batal;
- karena lewatnya waktu.

3.6 Konsep Tanda Tangan Dalam Transaksi / Akta

KUHPer (BW) hanya mengakui surat yang bertanda tangan, karena surat dalam BW diperlukan sebagai pembuktian di masa depan. Surat yang tidak bertanda tangan, tidak diakui dalam BW, karena 'tidak dapat diketahui' siapa penulisnya. Surat bertanda tangan itu disebut dengan 'akta'.

Orang pada umumnya akan berpendapat bahwa suatu akta sudah sepatutnya ditandatangani. Tandatangan ini menyebabkan orang yang menandatanganinya mengetahui isi dari akta yang ditandatanganinya. Orang tersebut juga terikat dengan pada isi dari akta tersebut[13].

Dalam BW, surat sebagai alat bukti tertentu dapat dibagi menjadi 2 bagian yaitu :

1. *akta bawah tangan* : dimana penandatanganan atas surat / akta tersebut dilakukan tidak di depan pejabat umum atau tidak ditandatangani oleh pejabat umum, sebagai mana dijelaskan dalam KUHPer pasal 1874, dan juga sebagian pada pasal 1869.
2. *Akta otentik* : dimana penandatanganan surat / akta tersebut dilakukan di depan pejabat umum atau ditandatangani langsung oleh pejabat

[13] *Ibid,Villmar, hal 478*

umum, sesuai pasal 1868 KUHPer. Akta otentik memiliki kekuatan hukum yang paling utama di depan hakim.

Pengertian akta sendiri sebenarnya adalah suatu surat yang diberi tandatangan, yang memuat peristiwa yang menjadi dasar daripada suatu hal atau perikatan, yang dibuat sejak semula dengan sengaja untuk pembuktian. Jadi untuk dapat digolongkan dalam golongan akta maka surat tersebut harus ditandatangani[14]. Keharusan akan adanya tandatangan dalam surat sehingga surat tersebut dapat disebut sebagai akat diatur dalam (pasal 1869 BW). Fungsi dari tandatangan disini adalah untuk memberi ciri atau mengindividualisir sebuah akta. Oleh karena itu nama atau tandatangan yang ditulis dalam huruf balok adalah tidak cukup, karena dari tulisan huruf balok itu tidak tampak ciri-ciri atau sifat-sifat dari si pembuat.

Yang dimaksud dengan penandatanganan adalah membubuhkan nama dari si penandatanganan, sehingga membubuhkan paraf, yaitu singkatan tandatangan saja adalah tidak cukup[15]. Nama itu harus ditulistangan oleh si penandatangan sendiri.

Dipersamakan dengan tandatangan pada suatu akta dibawahtangan ialah sidik jari (cap jari, atau cap jempol) yang dikuatkan dengan suatu keterangan yang diberi tanggal oleh seorang notaris atau pejabat umum lain yang ditunjuk oleh undang-undang. Notaris atau pejabat tersebut harus memberikan pernyataan bahwa ia mengenal orang yang membubuhkan sidik jari atau orang tersebut diperkenalkan kepadanya, dan bahwa isi akta itu telah dibacakan atau dijelaskan kepadanya, kemudian sidik jari itu dibubuhkan pada akta dihadapan pejabat tersebut (ps. 1874 BW, S.1867 no 29, 286 RBG)[16].

Pengesahan sidik jari dikenal dengan istilah ‘ *waarmerking’*, dan *waarmerking* ini berbeda dibandingkan dengan legalisasi [17].

Tandatangan yang dibubuhkan dalam suatu kontrak tidak harus dilakukan ‘secara langsung’ seperti seseorang membubuhkan tandatangan. Tandatangan itu bisa juga dalam bentuk stempel atau bentuk lainnya.

---

[14] *Sudikno mertokusumo, Hukum Acara Perdata Indonesia (Jogjakarta, penerbit Liberty;1993), hal124*

[15] *HR 17 Desember 1885,W 551,6 Mei 1910,W9025*

[16] *SEMA 10/1964 30 April 1964:suratkuasa dapat dibuat dibawah tangan asalkan saja sidik jari (cap jempol) dari sipemberi kuasa disahkan (dilegalisir) oleh KaPN, Bupati atau Wedana*

[17] *Selanjutnya baca S.1916 No.46 tentang waarmerking akta dibawahtangan dan S.1909 No 291 tentang legilasi tandatangan*

Syarat dari digunakannya tandatangan selain tandatangan ‘ konvensional’ adalah tanda tangan itu harus digunakan secara teratur. Keterangan / kontrak yang sudah dibubuhi ‘tandatangan’ tersebut lantas dianggap memang berasal dari orang yang tandatangannya tertera diatasnya dan orang tersebut lantas terikat oleh keterangan tersebut[18].

Tandatangan bukan merupakan bagian yang penting (substansi) dari suatu transaksi/ kontrak, tetapi kehadirannya dilihat atau diperhatikan karena keberadaannya atau bentuknya (*form*)[19].

Penandatanganan suatu dokumen secara umum mempunyai tujuan sebagai berikut :

1. Bukti (*evidence*) : suatu tandatangan akan mengotentifikasikan penandatangan dengan dokumen yang ditandatanganinya. Pada saat penandatangan membubuhkan tanda tangan dalam suatu bentuk yang khusus, tulisan tersebut akan mempunyai hubungan (*attribute*) dengan penandatangan [20].
2. Ceremony : penandatanganan suatu dokumen akan berakibat penandatangan akan tahu bahwa ia telah melakukan suatu perbuatan hukum, sehingga akan mengeliminasi kemungkinan adanya *inconsiderate engagement*[21].
3. Persetujuan (approval) : dalam pengunaannya dalam berbagai konteks baik oleh hukum atau oleh kebiasaan, tandatangan melambangkan adanya persetujuan atau otorisasi terhadap suatu tulisan, atau penandatangan telah secara sadar mengetahui bahwa tanda tangan tersebut mempunyai konsekuensi hukum [22].
4. *Efficiency and logistics* tanda tangan dalam suatu dokumen tertulis seringkali menimbulkan kejelasan dan keabsahan dari suatu transaksi dan juga akan mengurangi kebutuhan untuk mengecek keabsahan suatu dokumen kepada orang yang bersangkutan [23].

---

[18] *Ibid, Vollmar, hal 142*
[19] *Information Security Committee, Elektronic Commerce and IT Division America Bar Association, Digital signature Guidelines, (chicago:ABA,1996)*
[20] *Lon L.Fuller, Consideration andForms,799,800 (1941):Jeremy Bentam, The works of Jeremy Bentham, 508-585 (Bowring Ed,1962). Bentham menyebutkan tindakan membuat suatu bukti sbg preappointed (i.e made in advance evidence)*
[21] *John austin, Lectures on Jurisprudence (4th ed,1873)hal 939-944; Lon l.Fuller, hal 400:Rudolf von Jhering Geist Des rosmichen rechts (8th ed,1883(hal 494-498*
[22] *Model law on E-commerce, Uncitral 29th sess, pasal 17(1),UNDoc A/C.9/xxxix/CRP.i/Add.13 (1996)*
[23] *loc.cit,fuller, hal 801-882;loc.cit,Jhering, hal 494-497*

sedangkan dalam pasal 187 KUHP (kitab Undang-undang Hukum Acara Pidana, UU nomor 8 tahun 1981), disebutkan bahwa pengadilan juga menerima segala macam tulisan/ surat, baik tulisan/ surat yang bertanda tangan maupun yang tidak ditandatangani . Salah satu alasan untuk memasukan surat 'tak bertandatangan' dalam KUHAP adalah karena beberapa alat bukti tulisan mungkin bukan berupa 'perjanjian' tetapi bisa jadi merupakan 'daftar tembak' (*hit list*) yang ditemukan dalam proses penyidikan.

Penggunaan tandatangan didalam suatu akta adalah sangat penting, karena tanpa adanya tandatangan maka surat tersebut hanyalah bersifat sebagai surat belaka dan bukan bersifat sebagai akta.

3.7 Transaksi Elektronik Secara Umum

3.7.1 Defenisi

' Transaksi elektronik' kami definisikan sebagai berikut :

> *"segala data, informasi, atau catatan elektronik yang berkenan dengan dua orang atau lebih yang memiliki implikasi hukum"*

Yang kami maksud dengan 'berkenan' disini tidak berarti catatan itu harus dibuat oleh dua orang. Biarpun dibuat oleh satu orang, namun kalau sudah 'berurusan' dengan orang lain, catatan elektronik itu juga dapat dikategorikan sebagai 'transaksi elektronik'. Perhatikan hal ini mirip dengan perjanjian, dimana pada perjanjian bisa saja dibuat oleh satu orang, tetapi berakibat pada orang lain.

Jadi bisa kita simpulkan bahwa transaksi elektronik menurut definisi diatas, juga mencakup kontrak digital, dokumen-dokumen yang memiliki implikasi hukum dalam hard disk atau floppy disk, perintah transfer dana elektronik (misalnya pada EFT/ Elektronik Funds Transfer). Pesan-pesan (data messages) EDI / Electronic Data Interchenge, informasi pada website internet, electronic mail dan sebagainya.

Saat ini kita memfokuskan diri terlebih dulu pada pengaplikasian transaksi elektronik dalam perdagangan, karena dunia perdagangan paling banyak menggunakan transaksi elektronik. Dengan kata lain, dalam sub-bab ini kita berkonsentrasi dahulu pada masalah transaksi *electronic*

commerce.Meskipun demikian Seperti akan kita lihat dalam bab-bab selanjutnya,kita juga akan membahas masalah persengketaan yang melibatkan transaksi elektronik untuk persidangan non- perdata.

Disini kami juga berpendapat bahwa transaksi e-commerce pada dasarnya adalah salah satu bentuk dari perjanjian dalam bentuk elektronik. Meskipun informasi tersebut tidak ditandatangani,bukan berarti tidak terjadi perjanjian. Demikian juga kalau transaksi e-commerce tersebut hanya dibuat oleh salah satu pihak saja, tetap dapat dianggap sebagai perjanjian(ingat:perjanjian yang ditandatangani oleh satu pihak tetapi berakibat pada pihak lainnya.)

UNCITRAL[24] telah menetapkan suatu *mode*l law untuk *electronic Commerce* pada tahun 1996 yang kemudian direvisi pada tahun 1998. Model hukum tersebut berisi panduan- panduan yang disarankan diikuti oleh negara-negara anggota saat mereka membuat legislasi untuk e-commerce (atau transaksi elektronik secara umum). Adapun yang termaktub dalam model law tersebut antara lain adalah masalah :

- keberadaan dan pengakuan hukum transaksi elektronik,
- pengakuan konsep incorperation by reference
- jaminan keamanan atas keaslian transaksi elektronik dengan tanda tangan elektronik ataupun dengan cara lainnya yang dapat dipercaya dan diandalkan.
- Penggunaan salinan transaksi elektronik
- Pengarsipan transaksi elektronik
- Otomasi transaksi elektronik
- Hak dan kewajiban pengiriman transaksi elektronik dan penerima transaksi elektronik.
- Tanda penerimaan tanda bukti (*acknowledgement of receipt*) sebagai tanda untuk mengeksekusi transaksi .
- Kapan dikirim, diterima, terjadi dan berlakunya transaksi elektronik.

Patut dicatat sebenarnya model law ini sebelumnya dinamakan model law for EDI (*Elecronic Data Interchange*), namun pada saat saat terakhir diganti

namanya menjadi *model law for e- commerce* . meskipun demikian, prinsip-prinsip yang ada didalamnya juga dapat diterapkan untuk transaksi perdagangan elekronik secara umum.

Karena *model law* untuk *e-commerce* UNCITRAL telah memuat prinsip-prinsip umum yang cukup universal untuk berbagai jenis transaksi elektronik, maka pembahasan kami mengenai dasar-dasar transaksi elektronik akan mengacu kepada *model law* tersebut. Namun ,model transaksi elektronik lainnya yang tidak menggunakan EDI seperti penggunaan *web-wrap contract* dan *e-mail* di internet juga akan kami bahas.

3.7.2 Perjanjian elektronik

Salah satu bentuk dari transaksi elektronik yang menjadi perhatian kita adalah perjanjian dalam bentuk elektronik. Perjanjian di era digital akan menggunakan data digital sebagai pengganti kertas sebagai media dari perjanjian tersebut. Penggunaan data digital sebagai media dalam melakukan perjanjian akan memberikan efisiensi yang sangat besar terutama bagi perusahaan-perusahaan yang setiap bulannya banyak membuat perjanjian, seperti *trading house*, pabrik dan juga bagi perusahaan-perusahaan yang menjalankan bisnisnya di internet.

Namun, perjanjian elektronik terutama yang di internet memiliki berbagai permasalahan. Permasalahan itu antara lain adalah apakah suatu kontrak yang dilakukan secara *on-line* adalah *enforceable*, kapankah terjadinya kesepakatan, dan masalah penggunaan tanda tangan dalam perjanjian yang dilakukan secara *on-line*.

3.7.3 Pengakuan Hukum Atas Transaksi Elektronik

Salah satu aspek yang amat penting dalam transaksi elektronik adalah pentingnya pengakuan hukum atas suatu transaksi elektronik . Artinya, hukum tidak bisa nampikkan begitu saja bukti berupa transaksi elektronik di persidangan.Hal ini dijelaskan dalam *model law* untuk *e-commerce* UNCITRAL di pasal 5 . Masalah apakah transaksi elekronik itu terjamin keasliannya atau tidak, itu adalah masalah pembuktian dipengadilan.

---

[24] *http://www.uncitral.org*

Transaksi elektronik dalam pasal 6 juga diakui sederajat dengan ‘tulisan’ . Sekali lagi, masalah apakah transaksi elektronik itu terjamin keasliannya atau bukan, itu adalah masalah lain . Argumentasinya adalah tulisan biasa pun bisa asli, tetapi juga bisa palsu. Demikian pula halnya dengan transaksi elektonik dimana transaksi elektronik pun bisa terbuktikan keasliannya, atau sebaliknya terbukti palsu.

3.7.4 Konsep Incorporation by Reference

Dalam mengirimkan data-data elektronik, seringkali dilakukan penyederhanaan format data yang dikirimkan. Misalnya antara pabrik dengan supplier sering ada pertukaran data invoice, purchase order, payment instruction dan sebagainya. Kalau setiap pengiriman *message* tersebut harus mengetikan “Payment Instruction”, tentu akan memakan *bandwidth* (dengan kata lain, boros), sehingga dibuatlah kode untuk “Payment Instruction” misalnya “PAI”.

Untuk jelasnya kita lihat sebuah contoh invoice :

INVOICE

MYCO Ltd
123 High Road
Anyton
WESSEX WG7 5DT

Invoice No : A12345

Invoice date :12 Nov 1993

Purchaser
A. Buyer
17 Honeydew close
Middleton
WESSEX WG8 1DE

Invoice (if Other than purchaser)
Vaktrix Ltd
45 stonepark Rd
Middleton
WESSEX WG8 5HN

Order No : sales contact — Order Date — Terms
On-17462 Chas Meridith.tel:023-443678 — 93-11-11 — 28 days

Article No	Description	Number	Unit price	Cost
1935243	Transistor,pnp,ZTX502, 30volt,2 wTTS	6	0.27	1.62
1276097	Transistor,npn, BC107 equvalent	5	0.36	1.80
4563251	Capasitor,elecctr,500 microfard	8	0.84	6.72
2309812	Capacitor	1	3.50	3.50

	pack,assorted			
1549875	Resistor pack,preferred,values,0 .5 watt	2	1.75	3.50
			TOTAL	17.14

Gambar 20 contoh sebuah invoice[25]

Berdasarkan standar UN/EDIFACT (United Nations / EDI For Administration, Commerce and Transport), maka message EDI untuk invoice tersebut adalah :

UNH+MSGRF1+INVOIC:90:1:ZZ:EDMTRX'
BGM+380+A12345'
NAD+SE+++MYCO LTD+123 HIGT RD+ANYTON+WESSEX+WG7 5DT'
CTA+SR+:CHAS.MEREDITH+0123-443 678:TE'
NAD+BY+++.BUYER+17 HONEYDEW CLOSE+MIDDLETON+WESSEX+WG8 1DE'
NAD+IV+++VAKTRIX LTD+45 STONEPARK RD+MIDDLETON+WESSEX+WG8 5HN
PAT+09++931222:014'

UNS+D'
LIN+1++1935423:SA++:6PCS+0.27'
IMD+ZZZ+++TRANSISTOR,PNP,ZTX502,30VOLT,:2 WATTS'
LIN+2++1276097:SA++:5:PCS+0.36'
IMD+F+++TRANSISTOR,NPN,BC107 EQUIVALENT'
LIN+3++4563251:SA++:8:PCS+0.84'
IMD+F+++CAPACITOR,ELECTROLYTIC,500 MICRO:FARAD,25 VOLT'
LIN+4++2309812:SA++:1:PCS+3.50'
IMD+F+++CAPACITOR PACK,ASSORTED'
LIN+5++1549875:SA++:2:PCS+1.75'
IMD+F+++RESISTOR PACK,PREFERRED VALUES,:0.5WATT'
UNS+S'
TMA+17.14+++17.14'
UNT+21+MSGRF1''

Kalau kita perhatikan data message EDI di atas, banyak yang kode-kode yang harus diterjemahkan sehingga membuat data message EDI tersebut menjadi bermakna 'invoice' lengkap. *Kode-kode itu merujuk kepada* standar kode UN / EDIFACT atau ISO 9735. Berikut ini kami berikan contoh beberapa kode dengan maknanya.

UNB	Start of Interchange
UNG	Start of Group
UNH	Start of Message
UNT	End of Mesege
UNE	End of Group
UNZ	End of Interchange
UNS	Section Control

BGM	beginning of message
INVOICE	Invoice
NAD	Name and adrdress
CTA	Contact Information
PAT	Payment term
LIN	Line item
IMD	Item description

Tabel 4. Contoh incorporation by reference pada data messae EDI

Perhatikan bahwa kode-kode itu sendiri sebenarnya tidak bermakna apa-apa kalau tidak merujuk atau mengacu kepada standar tertentu. Dengan kata lain, kode-kode itu hanya bermakna kalau ada rujukan tertentu dari transaksi tersebut (atau diperjanjikan sebelumnya). Transaksi elektronik (dalam hal ini data message EDI) itu tidak bisa 'dimengerti' kalau tidak ada rujukan yang dianggap merupakan satu bagian dengan transaksi elektronik itu. Rujukan ke suatu dokumen tertentu inilah yang disebut dengan istilah *incorporation by reference*

Model law UNCITRAL menyatakan bahwa suatu transaksi elektronik tidak boleh ditolak maksud / makna sesungguhnya oleh hukum, hanya disebabkan karena transaksi tersebut memuat kode-kode yang perlu dirujuk ke dokumen lain. Perlu dicatat bahwa bukan hanya data messge EDI saja yang menggunakan incorporation by reference, namun juga banyak standar transaksi elektronik lainnya seperti untuk fund transfer (ISO 8583), kode-kode dalam HTML/WML/XML dan lainnya.

3.7.5 Tanda Tangan

Pasal 7 dari model law UNCITRAL menjelaskan mengenai pengakuan terhadap tanda tangan pada transaksi elektronik. Hanya saja 'tandatangan' itu harus terjamin keasliannya, sehingga penandatanganan dapat

diotentikasi oleh pihak lain. Pada sub-bab selanjutnya , kita akan membahas lebih banyak mengenai tanda tangan pada transaksi elektronik.

3.7.6 Keaslian Transaksi Elektronik

Jika ada jaminan bahwa informasi dalam dokumen elektronik itu diciptakan sampai saat ini dilihat kembali di masa depan, informasi itu tidak berubah, maka artinya kita dapat yakin bahwa dokumen elektronik tersebut terjaga keasliannya (atau keutuhannya, karena tidak berubah-ubah/terkutak katik). Hal ini dapat diimplikasi, jika ada suatu peraturan yang mengharuskan penyerahan suatu dokumen dan dokumen itu harus yang asli, maka transaksi elektronik dapat dianggap sama dengan dokumen asli. Model law dari UNCITRAL memuat masalah ini dalam pasal 8.

Kalau kita teliti pasal ini, ternyata yang digaris bawahi adalah informasi, bukan transaksi elektronik itu sendiri. Jadi informasi itu bisa berubah dari satu bentuk ke bentuk lain, asalkan *esensi* informasinya tidak berubah. Sebagai contoh :

- Dokumen kertas yang di scan dihadapan notaris, lalu diarsipkan ke dalam CD- ROM. Ini adalah contoh pengakuan keaslian dari benda fisik yang ditranformasikan ke wujud elektronik, asal informasinya dijamin keasliannya.
- Transaksi elektronik yang dicopy ke lokasi lain (dalam hal ini tidak ada perubahan wujud)
- Transaksi elektronik yang dikonversi dari satu format ke format lainnya. Misalnya konversi data message EDI dengan standar UN / EDIFACT ke standar ANSI X.12. proses konversi format tersebut harus menjamin bahwa informasi di dalamnya tidak berubah.

3.7.7 Pengarsipan dan Pencatatan Elektronik

Patut diperhatikan bahwa pasal 8 ayat 1b mengindiksikan pengakuan terhadap pengarsipan dan pencatatan secara elektronik (*electronic*

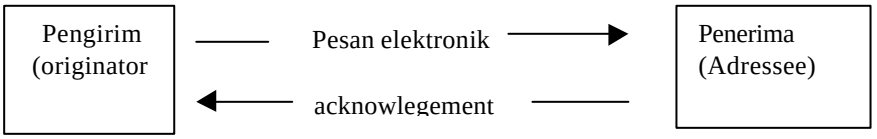
record) . Meskipun demikian, pasal 10 lebih menegaskan lagi pengakuan terhadap catatan elektronik. Arsip dan catatan elektronik dapat memenuhi persyaratan sebagai objek pengarsipan jika :

- Informasi dalam catatan elektronik dapat diakses. Hal ini jelas, karena tidak ada gunanya suatu catatan kalau tidak bisa diakses/ dibuka untuk dibaca di kemudian hari.
- Informasi dalam catatan elektronik itu dapat dijadikan referensi , artinya catatan elektronik tersebut harus bisa dirujuk kembali dengan jelas jika ada pihak lain yang ingin melihatnya kembali.

Sebenarnya ada suatu persyaratan (pasal 8 ayat 1b) berkenan dengan catatan elektronik, tetapi kami berpendapat bahwa persyaratan tersebut sangat terpaut dengan EDI jadi tidak bisa digeneralisasikan. Sebuah rekomendasi lain (pasal 8 ayat 1c), menyarankan agar sebaiknya transaksi elektronik yang direkam tersebut juga mendeskripsikan informasi pengirim, penerima, beserta waktu pengiriman dan waktu penerimaan diterima.

3.7.8 Komunikasi Transaksi Elektronik dan Terjadinya Kesepakatan

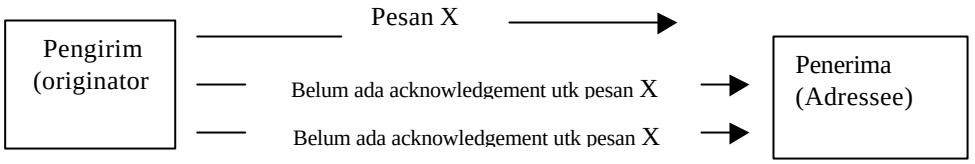
Secara umum, agar pengiriman pesan elektronik dari pengirim (*originator*) kepada penerima (*addessee*) dapat terjamin sampai kepada penerima, maka sang penerima sebaiknya mengirimkan pesan balasan (*acknowledgement*) yang memberitahukan kepada pengirim bahwa sang penerima sudah menerima pesan tersebut.



Gambar 21 Acknowledgement

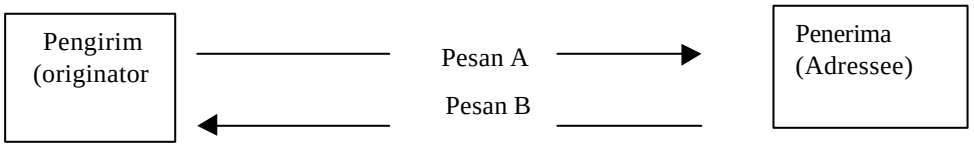
Hal ini amat penting, karena tanpa balasan dari penerima , sang pengirim tidak dapat memastikan apakah pengirim sudah bisa melaksanakan langkah selanjutnya sesuai kesepakatan diantara mereka berdua.

Jadi kalau tidak dibalas, maka pengirim akan menganggap bahwa pesan tersebut belum sampai dan akan mengirimkan pesan pemberitahuan kepada penerima bahwa belum ada pesan balasan (*acknowledgement*) yang sampai kepada pengirim kembali. Pemberitahuan ini akan dilakukan terus menerus sampai ada balasan dari penerima, atau samapi *time-out* (berhenti karena terlalu lama menunggu balasan).



Gambar 22 Pesan bahwa belum menerima acknowlegement

Pesan balasan yang diterima oleh pengirim, tidak harus berupa *acknowledgement* yang berupa pesan 'saya sudah menerima pesan anda'. Balasan yang diterima pengirim juga dapat berupa pesan lain yang merupakan *sequence* (kelanjutan) yang diharapkan dari pesan pertama. Dalam contoh dibawah ini, bisa saja pesan A berisi *purchase slip*, dimana jika penerima menerima *purchase slip* tersbut, maka penerima akan membalas *purchase slip* tersebut dengan mengirimkan pesan B yang berisi *payment instruction* kepada pengirim.



Gambar 23. Balasan berupa pesan lain yang bukan acknowledgement

Di sisi penerima pesan, sesudah menerima pesan dan sebelum melaksanakan kesepakatan berdasarkan pesan tersebut, memiliki hak untuk memeriksa *(verify*) keotentikan pesan elektronik tersebut, apakah benar dari pengirim yang dimaksud..

Pembahasan mengenai komunikasi transaksi elektronik amat penting karena berkaitan dengan kapan suatu perjanjian elektronik disepakati. Suatu perjanjian lahir pada detik tercapainya kesepakatan, maka perjanjian itu lahir pada detik diterimanya suatu penawaran (*offerte*) . Artinya dengan diterimanya suatu penawaran maka dapat disimpulkan bahwa kedua belah pihak telah mengetahui tentang adanya penawaran tersebut. Dan pihak penerima penawaran melakukan penerimaan terhadap penawar tersebut sehingga lahirlah suatu perjanjian.

Dengan tidak bertemunya antara orang yang memberikan penawaran dan orang yang menerima penawaran dalam suatu transaksi elektronnik, maka penawaran baru dianggap disepakati jika diterimanya jawaban atas penawaran (*acknowledgement*) oleh pemberi penawaran. Sehingga tampak jelas bagi kita bahwa kedua belah pihak tersebut dianggap telah sama-sama mengetahui adanya kesepakatan atas penawaran yang dijadikan patokan saat lahirnya suatu perjanjian.

Prinsip-prinsip komunikasi transaksi elektronik ini dibahs dalam bab ketiga dari model law untuk e-commerce UNCITRAL. Perlu kita perhatikan bahwa prinsip-prinsip komunikasi transaksi elektronik yang dibubuhi tanda tangan elektronik.

3.7.9 Pendelegasian Wewenang Kepada Komputer atau Orang Lain.

Sangat sulit dibayangkan apabila seorangg pejabat menandatangani ribuan dokumen export/import setiap bulannya. Namun kenyataannya, hal itu bisa terjadi. Untungnya dengan menggunakan komputer,proses pemeriksaan dokumen-dokumen acap kali bisa dipercepat.Dokumen export/import yang disetujui dapat segera dikirim kepada adressee.

Karena sesungguhnya bukan pejabat itu yang melakukan persetujuan (karena diotomatisasi oleh komputer), maka secara hukum perlu ada aturan yang memperbolehkan pendelegasian wewenang kepada komputer. Tentunya komputer tersebut harus diprogram terlebih dahulu sesuai dengan ‘kehendak; pemberi wewenang (dalam hal ini sang pejabat).Sang pejabat harus memiliki kontrol terhadap komputer yang melakukan pemeriksaan dan penyetujuan dokumen-dokumen export-import yang seharusnya ditandatangani oleh pejabat tersebut.

Pendelegasian wewenang juga dapat diperluas kepada orang lain (bukan komputer)

3.7.10 Jaminan Keamanan

Bab kedua dari *model law* UNCITRAL untuk e-commerce banyak menuntut adanya suatu jaminan atas kehandalan sistem, jaminan atas keaslian transaksi elektronik, atau metode pembuktian yang handal. Semua itu sebenarnya terkait dengan masalah keamanan (security) dari transaksi elektronik.

Secara hukum, keamanan transaksi elektronik dapat dicapai dengan cara :

a. Memberikan jaminan (atau serifikasi) kepada sistem, yang menunjukan bahwa sistem yang dipergunakan untuk transaksi elektronik tersebut dapat diandalkan keamanannya.
b. Mengimplementasikan sistem yang telah terbukti kehandalannya (misalnya sudah terbukti sulit di-hack). Jadi nanti kalau ada masalah di pengadilan, harus dibuktikan bahwa sistem tersebut keamanannya dapat diandalkan.

Masalah mengenai jaminan keamanan akan dibahas lebih lanjut pada bab pembuktian dan bab pengakuan standar (termasuk skim lisensi)

3.7.11 Shrink Wrap Contract dan Webwrap Contract

Shrink wrap contract biasanya banyak digunakan dalam suatu kontrak yang berkaitan dengan lisensi atas penggunaan suatu program komputer. Biasanya suatu program komputer dikemas didalam suatu kotak atau bungkus. Seorang pelanggang atau pembeli adalah tidak menandatangani suatu kontrak lisensi dengan *licensor*. Namun demikian ,lisensi atas penggunaan program komputer tersebut terdapat pada kotak kemasan program komputer tersebut. Lisensi atas penggunaan program komputer tersebut menyatakan bahwa apabila pembeli membuka kemasan tersebut maka ia dianggap telah menyetujui dan terikat dengan perjanjian lisensi tersebut.

Konsep dari *shrink wrap* contract ini adalah juga diadopsi didalam suatu perjanjian yang dilakukan secara on-line. Misalnya seorang penjual barang atau jasa hendak menawarkan barang atau jasanya kepada para

pelanggan. Penjual tersebut kemudian menampilkan ketentuan –ketentuan mengenai barang / jasa tersebut di dalam homepagenya. Ketentuan – ketentuan tersebut menyatakan bahwa calon pembeli setuju terhadap ketentuan-ketentuan tersebut maka ia tinggal menekan tombol [saya sepakat].

Penggunaan perjanjian dengan model webwrap ini merupakan suatu hal yang umum di internet. Webwrap ini disatu pihak memudahkan penjual maupun bagi pembeli namun disisi lain adalah memungkinkan terjadinya pelanggaran terhadap hak dan kewajiban pembeli.

3.7.12 E -mail

Penggunaan e-mail merupakan salah satu cara dalam membuat suatu kontrak. Penggunaan e-mail disatu sisi memudahkan, tetapi di sisi lain menimbulkan berbagai kerumitan. Permasalahan itu antara lain, tanpa pengamanan khusus seperti dengan digital signature, sebuah e-mail bisa dipalsukan. Namun dengan menggunakan digital signature, e-mail dapat dipergunakan sebagai perjanjian elektronik.

3.7.13 Pengakuan Transaksi Elektronik Dalam Hukum Indonesia

Perjanjian yang dibuat antar para pihak ini pada dasarnya tidak harus dibuat dalam bentuk tertentu (tertulis). Perjanjan –perjanjian yang ada pada galibnya berbentuk bebas. Perjanjian itu dapat diadakan dalam bentuk lisan dan apabila diterakan dalam suatu tulisan , itu sering kali mempunyai sifat alat pembuktian semata-mata[26] . Meskipun demikian terdapat beberapa perjanjian diisyaratkan adanya bentuk tertulis, bahkan diharuskan adanya akta notaris (hibah, pengesahan atas tanah yang terdaftar, pembentukan perseroan terbatas)

Syarat ‘tertulis’ dari suatu perjanjian berdasarkan pendapat diatas adalah sangat relatif dan hanya mempunyai sifat pembuktian semata. Pitlo dalam bukunya *Bewijs en Verjaring Naar het Netherlands Burgerlijk Wetboek*

[26] *HFA.Vollmar, pengantar Studi Hukum Perdata jilis 2 (jakarta, RajaGrafindo persada,1995), hal 128. Elips Pengembangan Hukum Ekonomi (jakarta:Elips,1998) hal 21*

memberikan definisi surat yang diberikan para ahli hukum pembuatan BW adalah ,

" pembawa tanda bacaan yang berarti, yang menerjemahkan suatu isi pikiran. Atas beban apa dicantumkannya tanda bacaan tersebut adalah tidak penting"

Dengan demikian, jika kita memperluas makna perjanjian kepada defenisi 'transaksi elektronik' yang kami buat, maka setidaknya ada dasar hukum bagi suatu transaksi yang menggunakan *media* elektronik

Perkembangan yurisprudensi di Indonesia pada saat ini juga telah menunjukan perkembangan yang baik, yaitu diterimanya *faxsimile* sebagai alat bukti dalam putusan Mahkamah Agung RI No.9K/N/1997[27]. Bukti berupa faxsimile dapat diterima sebagai bukti tulisan, perkembangan ini tentu sangat bagus dalam mendukung kegiatan bisnis pada saat ini.

Kemudian, berdasarkan Undang-undang nomor 8 tahun 1997 mengenai Dokumentsi Perusahaan, bab 3 pasal 12 sampai pasal 16, menyatakan bahwa dokumen yang ditransfer ke *microfilm* atau media lainnya dapat dianggap sama seperti dokumen aslinya, asalkan proses pengarsipan/pengtransferan tersebut dilegalisir oleh notaris.

Para pihak juga berwenang untuk mengadakan perjanjian apa saja yang akan berlaku sebagai bukti antara mereka (perjanjian bukti/perjanjian penetapan/ bewijsovreenkomst) seperti yang ada dalam *Arres* HR 3 Mei 1918[28]

Maksud dari perjanjian penetapan adalah perjanjian-perjanjian yang disitu ditetapkan, apakah yang akan merupakan hal yang menurut hukum bagi para pihak tanpa bahwa disitu ada maksud untuk menciptakan hak-hak dan/atau kewajiban-kewajiban baru[29]

Perjanjian ini tidak bersifat *obligator dan dispositif* tetapi *deklaratif* (menerangkan, menyatakan). Hal itu tidak menimbulkan sesuatu yang baru ,tetapi mempertetapkan apa-apa yang menurut penglihatan dari para pihak haruslah dipandang sebagai suatu perhubungan hukum yang ada. Perjanjian-perjanjian seperti ini adalah dimungkinkan dan sah berdasarkan

[27] Widjanarto, Dampak Implementasi Undang-undang Kepailitan Terhadap Sektor Perbankan' Jurnal Hukum Bisnis (vol 8,1999):79
[28] Vollmar,op.cit,hal 474
[29] Ibid,hal 135

aturan umum hukum perjanjian (*arres* HR 25 Juni1926, 2 Desember 1927,9 Januari 1941).

Sebagai contoh dua pihak yang bertransaksi dengan EDI, sebelum melakukan transaksi akan melakukan penandatanganan *trading partner agreement* dengan mempercayai *data message* yang saling dipertukarkan melalui sebuah EDI servis provider, sebagai bukti transaksi.

Apabila kita mengartikan syarat 'tertulis'secara harfiah maka perjanjian dalam bentuk elektronik sukar untuk dapat dimasukan dalam kategori ini. 'Tertulis' disini harus diartikan secara meluas, karena tidak selalu harus menggunakan media kertas. Jadi tertulis disini sebenarnya hanyalah salah satu media fiksasi saja atau perlekatan suatu informasi pada suatu media.

Sedangkan dalam perbuatan hukum lainnya secara umum bentuk tulisan hanya mempunyai arti sebagai alat bukti, yang hanya memperoleh arti sebagai alat bukti yang hanya memperoleh arti apabila perjanjiannya dibantah.

Berdasarkan pendapat tersebut diatas sebenarnya adalah tidak merupakan suatu masalah apabila suatu perjanjian itu dibuat/dituangkan dalam bentuk atom-atom tinta diatas kertas ('tertulis' dalam anggapan konvensional) ataupun dalam bentuk bit-bit data .

Hanya saja, kerancuan mengenai makna 'tulisan' itulah yang membuat transaksi elektronik sulit diakui, sehingga kata 'tertulis' ini haruslah diartikan secara meluas.

3.8 Transaksi Elektronik Dengan Tanda Tangan Elektronik

3.8.1 Tanda Tangan Digital

Penggunaan tanda tanngan digital (*digital signature*) adalah pendekatan yang dilakukan oleh teknologi *encryption* terhadap kebutuhan akan adanya suatu 'tandatangan' atau adanya 'penghubung' antara suatu dokumen / *data* / *messages* dengan orang yang membuat atau menyetujui dokumen tersebut . Penggunaan teknologi ini juga akan membantu para pihak untuk menyatakan bahwa suatu dokumen adalah sudah berupa dokumen yang '*final and binding*' .

Digital Certificate merupakan suatu sertifikat identitas milik seseorang yang berisi antara lain : nama, alamat, jabatan, *issuer*, dan berbagai informasi penting mengenai pemilik dari digital certificate tersebut. Pada saat ini

didunia pada umumnya standar yang digunakan untuk *public key certificate* adalah standar ISO/IEC/ITU X.509.

Fungsi dari *digital certificate* ini terutama adalah untuk menghubungkan (*securely associated*) antara sebuah *public key value* dengan seseorang , bagan hukum atau dengan sebuah alat/perangkat. Terdapat beberapa fungsi lain dari *digital certificate* ini, misalnya untuk menentukan kecakapan seseorang/badan hukum/perangkat. Penggunaan digital certificate ini memungkinkan para pihak identitas masing-masing pihak dan juga kecakapan dari para pihak melakukan suatu perbuatan hukum.

3.8.2 Tanda Tangan Elektronik

Apabila *digital signature* adalah suatu penerapan penggunaan *public key cryptography*, maka *electronic signature* adalah suatu teknik 'penandatanganan' yang menggunakan berbagai cara, artinya tidak harus menggunakan *public key cryptography*.

Defenisi atau penjelasan mengenai *electronic signature* menurut UNCITRAL *Uniform Rules on Electronic Signature Draft* adalah sebagai berikut :

(a) "Electronic signature" means data in electrinic form in, affixed to or logically associated with, a data message, and [that may be] used to [identity the signature holder in relation to the data message and indicate the signature holder's approval of the information contained in the data message]

(b) "enhanced electronic signature" means an electronic signature which [is created and] can be verified through the application of a security procedure or combination of security procedures that ensures that such electronic signature. :

(i) is unique to the signature holder [for the purpose for][within the contect in] which it is used;

(ii) can be used to identify objectively the signature holder in relation to the data message;

(iii) was created and affixed to the data message by the signature holder or using a means under the sole of the signature holder[30].

3.8.3 Perdebatan Penggunaan Istilah.

Sampai penulisan laporan penelitian tahap pertama ,kami belum memutuskan apakah kami akan menggunakan istilah 'digital signature' atau 'electronic signature' . Investigasi terhadap penggunaan istilah tersebut akan dilakukan pada fase kedua dari penelitian.

3.8.4 Kemungkinan Pengakuan Tanda Tangan Elektronik Dalam hukum Indonesia.

Cara untuk 'melihat' tanda tangan elektronik dalam perspektif hukum Indonesia adalah untuk melihatnya sebagai tanda tangan biasa. Jika kita mengasumsi bahwa transaksi elektronik dapat dianggap sama dengan tulisan (ayang diakui secara hukum), maka tanda tangan elektronik dapat dianggap sebagai suatu bentuk khusus dari transaksi. Dengan demikian , seluruh transaksi elektronik dengan tanda tangan elektronik dapat dianggap sebagai akta.

Kemudian dengan melihat karakteristik dari tanda tangan sebagaimana dijelaskan dalam sub bab 3.6, kita dapat menarik kesimpulan bahwa untuk dapat menerima surat tanda tangan (lebih tepatnya'penandaan') secara hukum, dalam sebuah teknik penandatanganan harus ada mekanisme untuk mengidentifikasi pihak yang melakukan penandatanganan dan mengidentifikasikan kesediaan dari pihak yang melakukan tanda tangan untuk sepakat dengan apa yang ditandatanganinya. Kalau tanda tangan elektronik dapat memenuhi syarat-syarat itu, maka tanda tangan elektronik dapat diterima sebagai tanda tangan yang valid.

Pada bab selanjutnya mengenai notarisasi, akan dibahas secara detail lagi syarat sebuah transaksi elektronik yang bertanda tangan dapat dianggap sebagai akta.

---

[30] *Uncitral, Working Group on Electronic commerce, Thirty-fourt session, Viena,8-19 February 1999, Draft on ELECTRONIC*

3.9 Pengakuan Transaksi Elektronik Secara Sektoral di Indonesia

Sebenarnya ada beberapa peraturan sektoral yang telah memberikan pengakuan eksplisit terhadap transaksi elektronik. Hal ini harus dilihat sebagai suatu inisiatif sektoral yang positif. Namun, tetap saja inisiatif tersebut memiliki kelemahan :

- Peraturan tersebut hanya berlaku secara sektoral dan tidak berlaku secara umum / lintas sektoral. Padahal dalam kenyataannya banyak transaksi-transaksi yang lintas sektoral. Contoh nyata adalah kasus EDI untuk export-import, dimana sebagian dokumennya sudah diolah secara elektronik. Hanya saja, bebrapa instansi tertentu yang terkait masih hanya mengakui data di atas kertas saja , dan tidak bisa menerima data elektronik.
- Peraturan –peraturan tersebut umumnya secara sederhana sekedar mengakui data / transksi elektronik. Artinya , tidak dibahas secara detail bagaimana cara membuktikan keaslian transaksi elektronik tersebut jika dijadikan alat bukti di pengadilan. Jadi tetap saja tidak memberikan jawaban yang defenitif apakah transaksi elektronik dapat dijadikan alat bukti di pengadilan.

Berikut ini kami jelaskan beberapa inisiatif peraturan sektoral yang memberikan pengakuan terhadap transaksi elektronik.

3.9.1 Bank Indonesia[31]

Dunia perbankan adalah salah satu sektor bisnis yang paling banyak menggunakan teknologi informasi. Tidaklah mengherankan jika teknologi informasi juga dimanfaatkan secara maksimal untuk mendukung sistem pembayaran nasional yang diselenggarakan oleh Bank Indonesia (BI).

BI telah mengimplementasikan Sistem Kliring Elekronik Jakarta (SKEJ) yang memungkinkan bank-bank peserta kliring untuk melakukan kliring secara elektronik. BI juga telah mengimplementasikan sistem Real Time Gross Settlement (RTGS) untuk mendukung pembayaran bernilai tinggi

---

SIGNATURES.

[31] *Informasi berdasarkan surat menyurat via e-mail dengan bpk Iwan Setiawan dari BI, 2 Mei 2001*

(*high value payment)* yang beresiko jika tidak dilakukan settlement segera / *real time*

Baik RTGS, SKEJ, maupun sistem kliring semi otomatis di daerah-daerah, telah menerima data dari bank peserta secara elektronik. Namun memang, warkatnya secara fisik masih dikirimkan. Tetapi seluruh proses settlement dilakukan dengan komputer secara elektronis.

Berkenaan pengakuan data elektronik, khusus yang terkait dengan sistem pembayaran, dalam Undang-undang Bank Indonesia, UU no 23 Tahun 1999, disebutkan dalam penjelasan pasal 16 tentang defenisi kliring yaitu

> *"pertukaran warkat atau data keuangan elektronik antar bak baik atas nama bank maupun nasabah yang hasil perhitungannya diselesaikan pada waktu tertentu…"*

Selanjutnya dalam Peraturan Bank Indonesia (PBI) No 1/3/PBI/1999 tanggal 13 Agustus 1999 tentang Penyelenggaraan Kliring Lokal dan Penyelesaian Akhir Transaksi Pembayaran Antar Bank Atas Hasil Kliring Lokal telah diatur lebih lanjut tentang 'pengakuan atas data elektronik sebagai dasar pembukuan, yaitu dalam Pasal 1 angka 8 yaitu

> *"Data Keuangan Elektronik yang selanjutnya disebut DKE, adalah data keuangan dalam bentuk elektronik yang digunakan sebagai dasar perhitungan dalam kliring lokal",*

juncto Pasal 2 ayat (3) yang menyatakan bahwa

> *'perhitungan kliring lokal dalam sistem semi otomasi dan elektronik didasarkan pada DKE"*

juncto pasal 10 ayat (1)

> *"DKE yang diperhitungkan dalam kliring lokal didasarkan pada warkat kliring dan (2) DKE dianggap sebagai data yang sah '*

Peraturan yang lain adalah PBI No 2/24/PBI/2000 tentang Hubungan Rekening Giro Antar Bank Indonesia Dengan Pihak Ekstern yang dalam

pasal 15 dan 19 mengatur perihal Penarikan Rekening Giro Rupiah dengan menggunakan sarana elektronik, yang dalam penjelasannya sarana elektronik didefinisikan sebagai "*suatu fasilits yang ditetapkan oleh BI dengan memanfaatkan teknologi komputer guna melakukan penarikan dana secara tunai dari satu rekening giro atau memindahkan dana dari satu rekening giro ke rekening giro lainnya".*

Sedangkan Pasal 21 nya mengatur tentang

" *penarikan atas rekening giro valas dengan pemindahbukuan menggunakan sarana Act. SWIFT dan teleks."*

3.9.2 Bapepam

Dunia pasar modal Indonesia mengalami perkembangan yang cukup signifikan. Hal ini dapat terlihat dengan maraknya isu akan berlangsungnya perdaganga saham secara on-line di Indonesia. Perdagangan saham melalui media elektronika dalam perkembangannya mulai diterapkan dalam sistem pasar modal Indonesia . Keberadaan perdagangan saham melalui media elektronik di bursa efek Indonesia ditandai dengan dipergunakannya *Jakarta Automatic Trading System* (JATS) yang diselenggarakan oleh Bursa Efek Jakarta (BEJ) dan demikian juga dengan Remote Trading yang dilaksanakan oleh Bursa Efek Surabaya (BES).

Berkenaan dengan hal tersebut, maka yang perlu ditelaah lebih lanjut adalah peraturan tentang pasar modal, yang memperbolehkan sistem perdagangan tersebut.

Peraturan perundangan pasar modal Indonesia pada dasarnya secara eksplisit tidak menjelaskan secara rinci sistem perdagangan yang akan digunakan nantinya.Hanya saja pada penjelasan pasal 1 butir 15 dan penjelasan pasal 55 Undang-undang Pasar Modal dinyatakan bahwa perdagangan melalui media elektronik lainnya dapat dilaksanakan . Dengan berbekal penjelasan tersebut maka transaksi perdagangan saham on-line secara legal dapat dilaksanakan. Hanya saja belum diatur tentang bagaimana tata cara pembuktian bahwa transaksi tersebut berlangsung, dan bagaimana bila terjadi perselisihan yang melibatkan data elektronik sebagai alat pembuktian nantinya.

3.9.3 Bea Cukai

Sejak tahun 1998 Direktorat Jenderal Bea Cukai Indonesia mengakui dan memakai sistem Elektronic Data Interchange (EDI) dalam melakukan tugasnya . Persatuan Bea Cukai Dunia atau World Custom Organization mewajibkan bagi anggotanya untuk menggunakan Sistem EDI khusus yang telah direkomendasikan dalam Colombus Declaration/ Deklarasi Kolombus tahun 1994 yaitu Rekomendasi 2 nomor 10,11,12, dan 13 serta rekomendasi 3.

Hal ini bertujuan untuk penyeragaman sistem dan harmonisasi sistem diantara instansi kepabeanan di masing-masing negara anggota, seperti yang diinginkan dalam *Kyoto Convention International Convention on the Simplification and Harmonization of Custom Procedures*. Penggunaan fasilitas Electronic Data Interchange (EDI) oleh Instansi Bea dan Cukai Republik Indonesia didasarkan pada peraturan :

1. Surat Edaran Ditjen Bea Cukai Nomor : SE-01/BC/1998 tentang Pendirian Warung EDI.
2. Surat Edaran Ditjen Bea Cukai Nomor : SE-13/BC/1998 tentang Tata Cara Pelayanan Elecronic Data Interchange (EDI) Kepabeanan dibidang ekspor.
3. Keputusan Ditjen Bea Cukai : KEP-33/BC/1999 tentang Penyelenggaraan Jasa Warung Electronic Data Interchange.

Dalam keputusan pasal 1 KEP-33 tahun 1999 yang dimaksud dengan Jasa Warung Electronic Data Interchange yang selanjutnya disebut Warung EDI adalah jasa pelayanan dalam rangka pertukaran data secara elektronik dari importir atau eksportir atau pengangkut atau kuasanya dalam mengirimkan atau menerima pesan elektronik kepabeanan ke atau dari komputer Kantor Pelayanan Bea dan Cukai melalui provider PT EDI Indonesia, yang meliputi :

1. penyiapan pemberitahuan pabean kepada Kantor Pelayanan Bea dan Cukai;
2. Pengiriman data pemberitahuan pabean melalui sistem EDI dan penyelesaian pemberitahuan tersebut;

3. Teknis operasional komputer yang berkaitan dengan penggunaan perangkat lunak EDI.

Pengusaha Pengurusan Jasa Kepabeanan (PPJK) adalah badan usaha yang melakukan kegiatan pengurusan pemenuhan kewajiban pabean untuk dan atas kuasa importir atau eksportir. PT EDI Indonesia menjadi penyedia jaringan pertukaran data elektronik di bidang kepabeanan antara importir, eksportir, pengangkut, PPJK dan masyarakat usaha lainnya dengan Direktorat Jenderal Bea dan Cukai.

Dalam pelaksanaannya ternyata banyak sekali permasalahan yang terjadi dimana, pengakuan transaksi melalui media elektronik telah diakui akan tetapi permasalahan mengenai identitas dari para pelaku masih belum jelas. Belum ada mekanisme yang menganggap keberadaan suatu identitas tidak dapat ditolak lagi, karena banyak pemalsuan identitas secara elektronik, dan belum mempunyai mekanisme verifikasinya.

Pelaksanaan transaksi EDI tersebut hanya berdasarkan perjanjian diantara lingkungan Importir (PIB). Transaksi EDI telah digunakan untuk Kepabeanan Soekarno Hatta dan Tanjung Priok.

3.9.4 Bea Materai Elektronik

Menurut undang-undang nomor 13 tahun 1985 mengenai bea materai, pasal 2 ayat 1, bea materai wajib dikenakan pada semua dokumen yang hendak dijadikan alat bukti di pengadilan perdata. Undang-undang tersebut juga menyatakan secara tegas di pasal 2 ayat 3 bahwa jika sebelum peradilan dokumen yang hendak dibawa ke pengadilan itu tidak wajib dikenakan bea materai, maka saat akan dibawa ke pengadilan, dokumen itu akan dikenakan bea materai.

Perkembangan terbaru dalam hukum Indonesia, seperti ditegaskan dalam Surat Keputusan Direktur Jenderal Pajak no 122.D/PJ/2000, mengizinkan teknik-teknik baru untuk menggunakan materai dengan sistem komputer . Hanya saja, yang diizinkan untuk menggunakan materai berbasis komputer hanyalah transaksi-transaksi yang memiliki nilai ‘uang’ sebagaimana dijelaskan dalam Peraturan no 24 tahun 2000 pasal 10.

BAB 4
PEMBUKTIAN

Transaksi elektronik yang dilakukan secara virtual (maya) sangat tergantung pada kepercayaan di antara para pihak yang terlibat. Hal ini terjadi karena aktivitas ber Internet adalah aktivitas yang maya yang berarti pihak-pihak yang berinteraksi tidak bertemu secara fisik. Untuk itu masalah pembuktian menjadi hal yang sangat penting, karena sangat riskan untuk mengandalkan hanya kepada kepercayaan untuk melakukan transaksi secara elektronik.

Teknologi tanda tangan digital (*digital signature*) benar-benar merevolusi dunia digital, sehingga memungkinkan untuk pertama kalinya sebuah dokumen elektronik ditandatangani secara elektronik pula. Hal ini amat penting karena jika ada persengketaan, dokumen elektronik itu akan diperlukan sebagai bukti.

Akan tetapi sarana pembuktian yang diterapkan pada transaksi elektronik tetap saja bersifat maya atau tak berwujud, karena terbentuk dari suatu proses elektronik. Sehingga dengan demikian diperlukan suatu pengkajian atau penelitian mengenai pembuktian dimana pembahasannya diawali dari masalah pembuktian yang telah dikenal dalam ilmu hukum dan diterapkan dalm praktek hukum sehari-hari. Setelah itu barulah dipadukan dengan permasalah pembuktian transaksi elektronik dan tandatangan elektronik.

4.1 Hakikat Pembuktian

Sebelum menapak lebih jauh, ada baiknya kalau kita meninjau terlebih dahulu hakikat dari pembuktian. Pada umumnya apabila kita menemui permasalahan dan harus mengambil keputusan yang tepat terhadap

permasalahan tersebut kita selalu berusaha untuk mengumpulkan berbagai masam fakta yang berkenan dengan permasalahan tersebut. Dengan fakta-fakta yang telah terkumpul kita gunakan untuk membuktikan permasalahan tersebut dan kita mencari pemecahannya. Dalam cabang-cabang ilmu pasti fakta-faka yang dikumpulkan guna menjadi bukti bagi suatu permasalahan sifatnya relatif pasti. Sebagai contoh, satu molekul air terdiri dari 2 atom hidrogen dan satu atom oksigen. Apabila komposisi tersebut diubah maka akan menimbulkan suatu zat baru lagi. Tidak demikian halnya dengan ilmu hukum yang merupakan salah satu cabang dari ilmu sosial. Pembuktiannya bersifat kemasyarakatan, karena walaupun sedikit terdapat unsur ketidakpastian. Oleh karena itu kebenarannya dapat dicapai merupakan kebenaran yang relatif. Kita harus memberikan keyakinan terhadap fakta yang dikemukakan itu harus selaras dengan kebenaran[32] .

Apabila untuk memutuskan suatu sengketa atau kasus mutlak hanya menyandarkan pada keyakinan hakim ini adalah hal yang sangat riskan karena dapat menimbulkan kekhawatiran bahwa keyakinan hakim tersebut akan bersifat subjektif, sehingga akan menimbulkan tindakan sewenang-wenang dari sang hakim yang justru tidak memberikan rasa keadilan bagi para pihak yang berperkara. Maka dari itu sewajarnyalah apabila dalil-dalil yang dikemukakan para pihak yang bersengketa menjadi pula dasar pertimbangan bagi hakim agar dapat dicapai suatu keputusan yang objektif. Dalam hubungannya dengan ari pembuktian, Prof Subekti berpendapat bahwa " *membuktikan ialah meyakinkan hakim tentang kebenaran dalil atau dalil-dalil yang dikemukakan dalam satu persengketaan"*[33]

Dalam hal ini kita coba ambil kesimpulan arti membuktikan. Membuktikan adalah upaya untuk mengumpulkan fakta-fakta yang dapat dianalisa dari segi hukum dan berkaitan dengan suatu kasus yang digunakan untuk memberikan keyakinan hakim dalam mengambil keputusan. Sedangkan pembuktian adalah proses untuk membuktikan suatu kasus yang disertai dengan fakta-fakta yang dapat dianalisa dari segi hukum untuk memberikan keyakinan hakim dalam mengambil keputusan.

---

[32] *Teguh Samudera, "Hukum Pembuktian Dalam Acara Perdata", Penerbit Alumni, 1992, hal 10*

[33] *Subekti Prof.SH. Hukum Pembuktian,cetakan ke-3, Pradnya Paramita. Jakarta, 1975, hal 5*

4.2 Pembuktian Dalam Acara Peradilan

4.2.1 Prinsip Pembuktian Dalam Acara Perdata

Alat –alat bukti yang diakui dalam peradilan perdata Indonesia diatur dalam HIR (*Herzien Indonesisch Reglement*) pasal 164 dan kitab Undang-undang Hukum Perdata (KUHPer) pada pasal 1866 yang berbunyi :

"Alat-alat bukti terdiri atas :

1. *bukti tulisan*
2. *bukti dengan saksi-saksi*
3. *persangkaan-persangkaan*
4. *pengakuan*
5. *sumpah"*

selain daripada apa yang telah disebutkan diatas HIR masih mengenai alat pembuktian lain yaitu hasil pemeriksaan setempat, seperti yang ditentukan dalam pasa-pasal berikut ini :

Pasal 153 (1) HIR yang berbunyi:

" jika ditimbang perlu atau ada faedahnya, maka ketua boleh mengangkat satu atau dua orang komisaris daripada dewan itu yang dengan bantuan penitera pengadilan akan melihat keadaan setempat atau menjalankan pemeriksaan di tempat itu, yang dapat menjadi keterangan kepada hakim."

Pasal 154 HIR (hasil penyelidikan seorang ahli) yang berbunyi :

> *" jika pengadilan negeri menimbang, bahwa perkara itu dapat lebih terang, jika diperiksa atau dilihat oleh orang ahli maka dapatlah ia mengangkat ahli itu, baik atas permintaan kedua pihak , maupun karena jabatannya."*

Tanpa mengabaikan pentingnya alat-alat bukti lainnya, pembahasan akan difokuskan terlebih dahulu kepada alat bukti tulisan. Hal ini disebabkan karena :

- Permasalahan yang menjadi perhatian saat ini adalah, kita perlu menjawab apakah dalam acara peradilan, dokumen elektronik dapat dianggap sama dengan surat yang telah kita kenal. Apakah kekuatan hukum dari dokumen elektronik tersebut sama dengan kekuatan hukum alat bukti surat dalam acara perdata ?
- Selain juga pada asasnya didalam persoalan perdata, alat bukti yang berbentuk tulisan itu merupakan alat bukti yang lebih diutamakan jika dibandingkan dengan alat bukti lainnya. Bahkan menurut definisi Prof. Mr. A. Pitlo, alat pembuktian adalah " *Pembawa tanda tangan bacaan yang berarti, menerjemahkan suatu isi pikiran*[34]

Alat bukti tulisan ini menurut doktrin ilmu hukum dan undang-undang secara garis besar di bagi menjadi 2 macam :

1. Tulisan biasa
2. Tulisan yang berupa akta. Tulisan yang berupa akta ini di bagi menjadi 2 yaitu :
    - Akta di bawah tangan.
    - Akta oetentik.

Dari pembagian seperti diatas hal yang menjadi perhatian adalah bilamana suatu tulisan dikatakan sebagai tulisan biasa dan bilamana dikatakan sebagai tulisan yang berupa akta. Pengertian akta adalah suatu surat di tanda tangani, diperbuat untuk dipakai sebagai alat bukti dan untuk dipergunakan oleh orang untuk keperluan siapa surat itu dibuat [35]

Selain itu yang termasuk dalam akta adalah : cek, tanda terima (kuitansi), surat perjanjian, atau surat apa pun yang dibuat dan ditanda tangani oleh orang yang berwenang dan disepakati oleh para pihak menjadi alat bukti.
Kemudian muncul berikutnya, kapankah akta tersebut disebut sebagai akta di bawah tangan dan kapan akta tersebut disebut sebagai akta otentik. Sesuai dengan ketentuan pasal 1868 Kitab undang-Undang Hukum Perdata (KUHAP Perdata) yang berbunyi :

[34] *Pitlo Prof.Mr "Pembuktian dan Daluwars" Penerbit PT Intermasa hal 51.*
[35] *Ibid , Hal 52*

"*Suatu akta otentik adalah suatu akta yang didalam bentuk yang ditentukan oleh undang-undang, dibuat oleh atau dihadapan pegawai-pegawai umum yang berkuasa untuk itu di tempat di mana akta di buat .*"

Maka untuk membedakan apakah akta tersebut akta otentik atau akta di bawah tangan yang harus kita perhatikan adalah dilihat dari terbentuknya akta tersebut, apabila akta tersebut dibuat dihadapan atau dibuatkan oleh pejabat yang berwenang (sebagai contohnya : notaris) maka akta tersebut adalah akta otentik. Apa bila akta tersebut tidak memenuhi hal di atas maka akta itu adalah akta di bawah tangan.

4.2.2 Prinsip Pembuktian Dalam Acara Pidana

Dalam hukum pidana yang ingin dicapai ialah kebenaran meteril. Menurut Wirjono, bahwa kebenaran itu biasanya hanya mengenai keadaan-keadaan tertentu pada masa lampau[36]. Disitulah kesulitannya, suatu peradilan mengungkapkan suatu fakta di masa lampau, tidak mungkin tercapai.

Dalam mencari atau menelusuri kebenaran sejati dalam hukum acara pidana kita bukanlah hal yang sederhana. Maka hukum acara pidana hanya dapat menunjukan jalan untuk mencari sebanyak mungkin persesuaian antara keyakinan hakim dengan kehadiran alat bukti dan barang bukti.

Membicarakan mengenai pembuktian dalam hukum acara pidana tentunya tidak dapat meninggalkan dari ketentuan hukum mengenai alat bukti dan barang bukti yang ada di dalam KUHAP, mengingat alat bukti dan barang bukti menjadi dasar untuk memutus perkara pidana (dari pasal 183-189 KUHAP), dan barang bukti dalam pasal 39 KUHAP

Menurut pasal 184 KUHAP alat bukti antara lain adalah :

1. *Keterangan saksi*
2. *Keterangan ahli*
3. *Alat bukti surat*

[36] *mertiman Prodjohamidjojo,SH. Pembahasan Hukum Acara Pidana, dalam teori danpraktek, Jakarta:Pradnya Paramita, hal 133*

4. *Petunjuk*
5. *Keterangan terdakwa.*

Pasal ini bersifat limitatif, artinya penggunaan alat bukti tersebut hanya yang disebutkan dalam pasal tersebut saja.

Dalam pasal 183 KUHAP, seorang hakim dapat memutus perkara dengan berdasarkan minimal dua alat bukti (syarat minimum pembuktian) .Selanjutnya dengan bekal alat bukti yang ditemukan itu, hakim tersbut akan memperolah keyakinan bahwa memang telah terjadi suatu tindak pidana. Jika kita cermati rumusan pasal 183 KUHAP tersebut, dengan dua alat bukti tersebut belumlah cukup bagi hakim untuk menjatuhkan pidana kepada seseorang, karena masih diperlukan keyakinan hakim atas dua alat bukti yang dihadirkan disidang pengadilan. Jika dengan minimal dua alat bukti tersebut hakim memperoleh keyakinan, maka berdasarkan pasal 183 dan 184 KUHAP pelaku tindak pidana dapat dijatuhkan hukuman sesuai dengan perundang-undangan yang berlaku.

Dalam hukum acara pidana di Indonesia, alat bukti (184 KUHAP) dan barang bukti (39 KUHAP) yang masih terbatas yang disebutkan di dalam undang-undang, karena kita menganut sistim pembuktian negatif (*negatief wettelijke*), yaitu seseorang tidak dipidana tanpa adanya suatu keyakinan hakim terhadap alat bukti yang diketemukan yang sesuai dengan undang-undang.

4.3 Pembuktian Transaksi Elektronik Dalam Acara Perdata

4.3.1 Pembuktian Transaksi Elektronik Biasa

Ada yang berpendapat bahwa transaksi elektronik tanpa tanda tangan eletronik, kekuatan hukumnya sama dengan ucapan lisan. Artinya, selama pihak yang tersangkut dengan transaksi elektronik tersebut merasa bahwa tidak ada permasalahan, maka perjanjian dalam transaksi elektronik itu mengikat. Namun akan terjadi masalah besar kalau terjadi perselisihan mengenai transksi elektronik tersebut.

Pengkajian Hukum Tentang Masalah Kekuatan Hukum Alat Bukti Elektronik, BPHN Departemen Kehakiman RI Tahun 1996/1997

Selain itu ada juga yang berpendapat bahwa transaksi elektronik jenis ini dapat dimasukkan sebagai tulisan biasa setelah diperkuat terlebih dahulu oleh saksi ahli. Alasannya adalah :

- Berbeda dengan lisan, transaksi elektronik tanpa tanda tangan digital tetap merupakan sesuatu yang bisa di-*retrive* ulang dalam bentuk aslinya.
- Meskipun tidak menggunakan tanda tangan elektronik, bisa jadi transaksi elektronik itu menggunakan tehnik kriptografi kunci simetrik. Untuk beberapa jenis aplikasi, sebenarnya pengamanan dengan kunci simetrik bisa saja mencukupi kebutuhan dan bisa jadi cukup aman. Oleh karena itu, dalam pembuktian transaksi elektronik yang diamankan dengan kunci simetrik, bisa saja menggunakan saksi ahli untuk merperkuat bukti.
- Menurut para penulis BW, surat dapat ditulis pada media apapun. Kami menginterpretasikan bahwa termasuk media elektronik dapat dijadikan ‘ tempat menulis’.

Beberapa pendapat lain mengatakan bahwa transksai elektronik hanya sama dengan perjanjian tidak tertulis / lisan, karena data elektronik dapat diubah-ubah dengan mudah. Kami berpendapat bahwa pendapat ini bukanlah argumentasi yang baik, karena seseorang juga dapat dengan mudah melakukan manipulasi dokumen (bahkan dokumen yang tertandatangani).

Salah satu alasan lain untuk menolak transaksi elektronik sebagai alat bukti meskipun dari sudut pandang sosiologis- adalah karena masyarakat sudah sangat terbiasa dengan kertas dan tinta, sehingga untuk membiasakan agar masyarakat (dan pengadilan) mau menerima trasaksi elektronik agak sulit dan membutuhkan ‘waktu’

4.3.2 Pembuktian Tanda Tangan Elektronik

Sebenarnya dalam sistem hukum kita juga sudah dikenal suatu konsep keamanan untuk perdagangan yang agak mirip dengan konsep kriptografi kunci publik (penekanan pada kosep pasangan / pairs). Zaman dahulu, untuk keperluan otentikasi dengan mitra dagang, dipergunakan tongkat

kayu yang dipatahkan menjadi dua. Jika orang hendak melakukan pencacahan atas suatu transaksi, orang menorehkan sebuah goresan yang mengores sambungan kedua tongkat (yang berpasangan) tersebut. Untuk mencocokkan, cukup dengan menyambungkan kedua tongkat tersebut dan melihat apakah goresan ini 'melintas' sambungan/patahan tongkat dengan baik.

Hal ini dapat kita lihat pada bunyi pasal 1887 Kitab Undang-undang Hukum Perdata (KUHAP Perdata) yang berbunyi :

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

Namun menurut pendapat kami, penggunaan pasal tersebut untuk tanda tangan elektronik kurang kuat.

Seperti yang telah dijelaskan sebelumnya bahwa suatu tulisan, dalam hal ini berwujud dokumen, akan menjadi suatu akta apabila tulisan atau dokumen tersebut dibubuhi tanda tangan dan akan menjadi akta otentik bila dibuat di hadapan atau oleh pejabat notaris.

Yang menjadi masalah, apakan tanda tangan digital tersebut mempunyai makna atau fungsi atau bahkan kekuatan hukum yang sama dengan tanda tangan konvensianal ? Ada dua point yang harus diperhatikan sebelum kita menjawab pertanyaan ini :

- Kita harus ingat bahwa fungsi hakiki dari tanda tangan konvensional dalam suatu dokumen (perjanjian) adalah untuk membuktikan keberadaan dari para pihak yang terlibat dalam perjanjian.Maksudnya kalau ada sengketa (atau permasalaah yang berkenaan dengan dokument tersebut) maka dapat dibuktikan keberadaan para pihak yang menandatangani dokumen tersebut dan menjadi suatu perwujudan kesepakatan terhadap isi dokumen yang bersangkutan.

- Kemudian, sebenarnya yang kita inginkan adalah agar tanda tangan elektronik memilik kesamaan keberadaan hukum dengan tanda tangan konvensional pada kertas.

Jadi untuk mengakomodir kedua point di atas, kami mengusulkan agar keberadaan hukum transaksi elektronik yang bertanda tangan elektronik diperlakukan sama dengan akta (baik akta bawah tangan maupun akta otentik) *selama sekuriti (keamanan) dan keontentikan dari tanda tangan elektronik tersebut dapat dibuktikan di pengadilan.* Otentik di sini artinya benar bahwa pihak yang menyepakati transaksi elektronik tersebut memang 'menandatangani' transaksi elektronik tersebut.

Bisa saja pendapat kami ini dibantah karena tanda tangan dalam akta bawah tangan saja (dimana penandatanan dilakukan tanpa disaksikan pejabat umum) dapat diterima dipengadilan (kecuali juka dibuktikan sebaliknya). Namun mengapa tanda tangan elektronik-yang relatif lebih aman ketimbang tanda tangan biasa-harus dibuktikan dahulu keasliannya didepan pengadilan ?. Menurut kami, hal itu tetap untuk mengakomodir rendahnya akseptansi sosial terhadap tanda tangan elektronik.

Ada beberapa cara yang dapat kami usulkan untuk membuktikan keberadaan tanda tangan elektronik sehingga mendapatkan pengakuan awal sebelum proses pengadilan berlangsung. Artinya,keaslian tanda tangan elektronik itu langsung dapat diakui di pengadilan (presumption) kecuali ada yang bisa membuktikan sebaliknya (pembuktian terbalik)

Salah satu cara yang banyak digunakan berbagai negara adalah dengan cara melakukan audit dan memberikan lisensi pemerintah terhadap infrastruktur yang dipergunakan untuk 'membuat' tanda tangan elektronik.Lisensi tersebut memberikan jaminan bahwa infrastruktur tersebut telah diaudit dan memenuhi syarat minimun yang ditetapkan pemerintah. Dalam banyak kasus yang diberi lisensi adalah CA-nya. Oleh karena itulah, tanda tangan yang dihasilkan oleh infrastruktur kunci publik yang disediakan oleh CA yang berlisensi seharusnya dapat langsung diterima dipengadilan tanpa perlu dibuktikan keasliannya . Pada bab berikutnya, kita akan melihat bagaimana skim lisensi dari pemerintah ini berkaitan dengan masalah akta otentik.

4.4 Pembuktian Transaksi Elektronik Dalam Acara Pidana

4.4.1 Pembuktian Dalam Pidana Komputer

Usaha yang dilakukan oleh BPHN pada tahun 1996/1997 dibawah pimpinan Koesparmono Irsan[37] secara keseluruhan tidaklah merubah (menambah atau mereduksi) alat bukti yang terdapat didalam pasal 184 KUHAP. Namun dari penelitian (kajian) yang dilakukan oleh tim BPHN, bukti elektronik tersebut dapat menjadi bahan pertimbangan bukti elektronik tersebut dapat menjadi pertimbangan bagi hakim dalam memutus suatu perkara. Permasalahan besar penggunaan bukti elektronik adalah kekuatan pembuktian dari bukti elektronik tersebut.

Wacana bukti elektronik bukanlah hal baru dalam kejahatan di Indonesia yang memanfaatkan komputer. Pangkajian masalah pembuktian dalam tulisan ini, mencoba membandingkan dengan praktek di beberapa negara, khususnya inggris.

Bagian yang harus diperhatikan sebelum tiba pada taraf pembuktian adalah pencarian alat atau barang bukti yang mungkin ada (diketemukan). Kemudian harus dilakukan suatu *due diligent* terhadap sistem komputer. Hasil dari pemeriksaan awal atas keabsahan suatu sistem komputer tersebut (dapat berupa sertifikat, atau surat keterangan lainnya yang ditanda tangani oleh pejabat yang berwenang) nantinya akan menjadi suatu jaminan bagi pihak lain yang telah melakukan suatu aktifitas dengan menggunakan sistem komputer tersebut. Semua data dan informasi yang dihasilkan oleh komputer bersertifikat tersebut tentunya dapat dipertangungjawabkan.

Jika di kemudian hari terjadi suatu sengketa, maka bukti elektronik yang ada didalam *harddisk, disket* atau hasil *print out*, memiliki kekuatan pembuktian yang sempurna. Sertifikat atau surat keterangan bekerjanya sistem tersebut, dijadikan sandaran bahwa peralatan komputer tersebut aman dan dapat dipercaya.

4.4.1.1 Jenis Bukti Elektronik

Bukti elektronik terdiri 3 macam :

1. Real evidence

Bukti elektronik yang dimaksud disini adalah; hasil rekaman langsung dari suatu aktifitas elektronik, hasil penghitungan atau analisa oleh suatu sistem komputer yang telah bekerja sesuai dengan prosedur perangkat lunak yang digunakan untuk pemrosesan data atau informasi, rekaman data log dari sebuah server dalam Internet, atau juga dapat berbentuk salinan (*receipt*) dari suatu peralatan seperti hasil rekaman kamera yang menggunakan sensor. *Real evidence* ini dapat digunakan dalam banyak kemungkinan. Kita ambil contoh sebuah bank melakukan suatu transaksi dengan nasabah tentang pemotongan pajak sekian persen secara otomatis atas rekening, dan setiap waktu (jam,hari, minggu, dst) nasabah tersebut dapat mengeceknya, maka pemotongan (penghitungan) pajak tersebut termasuk dalam real evidence.

2. Hearsay evidence

   Kemudian yang kedua adalah *hearsay evidencce*, dimana dokumen atau rekaman yang merupakan hasil dari pemrosesan dengan menggunakan komputer yang kesemuanya adalah salinan atas sebuah informasi diatas kertas. Pemrosesan data komputer tersebut tidak berlangsung secara otomatis melainkan dilakukan oleh manusia.

   Contohnya adalah dalam suatu transaksi dibank, seorang nasabah hendak menguangkan (menukarkan) sebuah cek pada sebuah bank, kemudian data yang tertera diatas cek tersebut *divalidasi* dengan menggunakan komputer yang ada di bank tersebut. Apakah benar tanda tangan se pemilik rekening, nomor rekeningnya, dan identitasnya, maka salinan cek setelah melewati proses *validasi* tersebut dapat digolongkan kedalam *hearsay evidence*. Penggunaan bukti elektronik tersebut didalam pengadilan nantinya harus diperkuat oleh alat bukti dan bukti lainnya.

3. Derived evidende [38]

   Penggolongan yang terakhir adalah, kombinasi antara keduanya (real evidence dan hearsay evidence) Penggunaan data atau pesan elektronik sebagai barang bukti di pengadilan di cari ada tidaknya suatu

[38] *Benjamin Wright,The Law of electronic EDI, E-mail and Internet technology, Prof, And Liability, Second Edition, hal 143.*

hubungan antara keduanya. Contohnya dalam suatu transaksi di bank, setiap harinya dilakukan singkronisasi transaksi (*balancing*) antara data yang merupakan rekaman langsung suatu aktifitas suatu transaksi dengan menggunakan komputer dengan aktifitas para pihak (bank dengan nasabah).

Sebenarnya dari ketiga penggolongan bukti elektronik ini yang menjadi pokok masalah adalah sejauh mana bukti elektronik tersebut dapat mendekati kebenaran materil dari sengketa yang dimaksud.

4.4.1.2 Panduan penggunaan bukti elektronik

Menurut pendapat kami, ada tiga hal yang dapat dijadikan panduan untuk menggunakan bukti elektronik dalam suatu sengketa yang terjadi dalam transaksi elektronik :

1. Adanya pola (modus operandi) yang relatif sama dalam melakukan tindak pidana dengan menggunakan komputer.
2. Adanya persesuaian antara satu peristiwa dengan peristiwa yang lain.
3. Adanya motif (alasan melakukan tindak pidana)

4.4.1.3 Jalur Pembuktian

Masih menggunakan contoh dari sistem hubungan Inggris, ada beberapa cara agar suatu transaksi elektronik dalam pengandalian pidana dapat diterima menjadi bukti [39] ;

1. The real evidence route

Bukti elektronik sebagai suatu alat bukti yang sah dan yang berdiri sendiri (*real evidencce*) tentunya harus dapat memberikan jaminan bahwa suatu rekaman / salinan data (*data recording*) berjalan sesuai dengan prosedur yang berlaku (telah dikalibrasi dan diprogram) sedemikian rupa sehingga hasil *print out* suatu data dapat diterima dalam pembuktian suatu kasus.

2. *The statutory route*

Kemudian dengan berpangkal suatu penetapan atau pengesahan atas suatu data (*statutory route*) suatu bukti elektronik dapat diterima sebagai alat bukti di pengadilan. Contonya adalah perkara (*collins v Carnegie*) dimana dalam kasus tersebut dikedepankan salinan dokumen berupa ijazah, dengan pertimbangan bahwa dokumen tersebut merupakan dokumen publik. Pihak yang memiliki kewenangan untuk mensahkan dokumen atau data tersebut adalah negara atau pengadilan. Berdasarkan *Police and Criminal Evidence Act 1984* section 23 dan 24, dalam hal pembuktian suatu kasus, keabsahan data/dokumen tidak harus tercetak diatas kertas tapi juga termasuk data atau informasi yang ada dalam sebuah disket, dokumen yang diterima dengan menggunakan komputer melalui fasilitas telekomunikasi (faks,e-mail) sepanjang dapat dibuktikan data/informasi itu asli (original) atau hasil foto copy yang otentik, kemungkinan data atau informasi tersebut dapat diterima. Pada kategorisasi ini yang ditetapkan adalah data atau informasi tersebut dapat diterima. Pada kategorisasi ini yang ditetapkan adalah data atau informasi yang ada di dalamnya, atau data tersebut dinyatakan otentik.

3. *The expert witness*

Selanjutnya dalam peranan saksi ahli (*the expert witness*) tidak berbeda dengan yang ada di dalam perundang - undangan kita (UU no.8 tahun 1981 KUHAP) bahwa keterangan seorang ahli dapat menjadi alat bukti terhadap suatu kasus, dimana keterangan yang diberikan berdasarkan pada pengetahuan dan pengalaman. Kesaksian yang diberikan akan menjadi bahan pertimbangan bagi hakim terutama mengenai kekuatan pembuktian suatu alat bukti dan memberikan suatu standar keakuratan dan keobjektifan bekerjanya suatu sistem komputer.

[39] *martin Wasik, crime and the computer (new york :oxford University press) 1991 hak 172-183*

Singkatnya, jika terjadi suatu kasus penggunaan komputer secara ilegal maka seorang ahli di dalam suatu persidangan dapat dipanggil kemudian saksi tersebut memberikan keterangan mengenai cara kerja dan sistem komputer.

Ketiga pola ini tidak dijelaskan apakah harus selalu ada dalam pemeriksaan suatu kasus didalam pengadilan. Namun jika kita lihat lebih lanjut, bahwa keberadaan data elektronik akan sangat lemah tanpa didukung oleh ketiganyasecara bersamaan, mengingat tidak semua sistem komputer telah melewati proses kalibrasi (merujuk pada real evidence) atau belum adanya keseragaman mengenai penggunaan *hearsay evidence* dalam suatu kasus disetiap daerah, sehingga membutuhkan penetapan lebih lanjut dari pengadilan atau pihak yang berkepentingan (contohnya adalah negara yang memberikan penetapan suatu ijazah dalam bentuk elektronik)

Dari gambaran yang diberikan oleh peraturan di Inggris tersebut, kiranya dapat dipadukan dengan apa yang ditentukan oleh perundang-undangan kita, dalam hal ini adalah KUHAP. Dalam KUHAP kita perihal alat bukti bersifat limitatif, hanya terbatas pada apa yang disebutkan dalam pasal 184 KUHAP.

Alat bukti elektronik tidak dikenal dalam KUHP. Namun demikian tidak berarti bila terjadi suatu perkara kejahatan dengan menggunakan komputer pelaku kejahatan tersebut lolos dari jeratan hukum. Dalam kejahatan komputer, ketentuan pasal 183 KUHAP dapat diterapkan meskipun perlu pembuktian lanjut. Alat bukti yang mungkin ditemukan dalam suatu transaksi jika, berdasarkan pasal 184 KUHAP; keterangan saksi, keterangan ahli, surat petunjuk dan keterangan terdakwa.Namun biasanya keterangan saksi sangat sulit untuk diperoleh, mengingat pelaku tindak pidana ini biasanya melakukan aksinya secara sendirian. Paling mungkin jika terjadi penyerataan, maka antara pelaku dapat menjadi saksi bagi yang lainnya.

Mengenai alat bukti surat yang diketemukan, maka penuntut umum dapat menggunakan alat atau barang bukti tersebut sebagai dasar untuk menuntut terdakwa.Kemudian bukti surat (*fax, receip, e-mail*) sepanjang

dapat dipastikan bahwa suatu komputer bekerja dengan baik dan dapat dibuktikan keobjektifannya. Dalam pasal 187 (a,b) KUHAP, dikatakan bahwa surat tersebut harus dibuat didepan pejabat yang berwenang atau orang yang memiliki suatu pekerjaan tertentu. Kita ambil contoh; jika seorang dokter (orang yang memiliki tangung jawab profesi) membuat suatu resep untuk pasiennya dengan menggunakan surat elektronik ***(e-mail***). Ternyata apa yang tertera di dalamnya justru membuat si pasien bertambah parah, karena meminm obat yang diberikan oleh dokter melalui ***e-mail*** tersebut. Dalam kasus tersebut, apakah si dokter tidak dapat melarikan diri dari tanggung jawab. Jika dapat, sangat tidak adil sekali bagi si pasien.

Contoh lain, seorang notaris (pejabat yang berwenang) mengesahkan suatu akta tanah, yang dikirim melalui faks, kemudian disisi lain ada pihak yang merasa keberatan atas hasil faksimili tersebut. Menurut kami, sepanjang dapat dibuktikan keotentikan (original) akta tersebut maka surat tersebut dapat dijadikan alat bukti.

Melihat contoh hukum yang berlaku di Inggris, dalam sebuah kejahatan dengan menggunakan komputer, keterangan ahli sangat berperan sekali dalam memberikan pertimbangan pada hakim, apakah suatu sistem komputer bekerja dengan baik. Meskipun pendekatannya akan bersifat teknis, tapi hal itu akan memperkuat alat bukti lain yang diketemukan.

4.4.1.4. Penggunaan KUHAP Dalam Pidana Komputer

Berawal dari penggunaan bukti petunjuk yang bersumber, sebuah petunjuk dapat diperoleh dari keterangan saksi, surat dan keterangan terdakwa (pasal 188(2) KUHAP). Bila keterangan saksi dan keterangan terdakwa tidak diketemukan, maka petunjuk dapat diperoleh dari surat atau dokumen yang diketemukan, yang tentunya diketemukan persesuaian satu dengan lainnya mengenai alat bukti tersebut. Jika terdapat keamanan bentuk, metode atau cara dalam melakukan suatu kejahatan komputer (contoh:*hacking* komputer) maka dari situ akan diperoleh petunjuk (bukti

awal) yang nantinya tetap harus dibuktikan dengan bantuan seorang ahli untuk menjelaskan kasus tersebut.

Berdasarkan uraian diatas, maka syarat minimun pembuktian dalam pasal 183 KUHAP, dalam memutus suatu perkara sekurang-kurangnya terdapat dua alat bukti yang sah seorang hakim memperoleh keyakinan. Di mana diperoleh alat bukti keterangan ahli, surat dan petunjuk. Namun memang harus diakui keberadaan alat bukti elektronik tidaklah dapat berdiri sendiri sebagai alat bukti (*real evidence*) melainkan harus didukung, oleh alat bukti lain. Bekerjanya suatu sistiem komputer sesuai dengan satndar merupakan syarat mutlak untuk dapat diterimanya alat bukti elektronik sebagai alat bukti yang sah dipengadilan. Bukan masalah yang sederhana ,"keontentikan" suatu data yang diketemukan dalam operasional komputer memang menjadi sandaran, untuk menyatakan bahwa suatu aktifitas komputer tersebut tidak bertentangan dengan undang-undang.
Pengaturan barang bukti di dalam peraturan perundangan kita, khususnya adalah pasal 39 KUHAP, dimana membedakan ;

- barang yang di gunakan untuk melakukan tindak pidana
- barang yang digunakan untuk membantu tindak pidana
- barang yang merupakan hasil dari suatu tindak pidana
- barang yang diperoleh dari suatu tindak pidana
- informasi dalam arti khusus

Tidak diaturnya mengenai alat bukti elektronik didalam KUHAP kita menyebabkan bukti elektronik kedudukannya menjadi tidak sederajat dengan alat bukti lainnya. Sangat logis ketika memang adanya suatu jaminan atas suatu data atau informasi yang ada, karena mungkin diadakan perubahan oleh orang lain. Dalam perundangan kita data elektronik dapat dimasukkan kedalam suatu barang bukti atau informasi dalam arti khusus. Keberadaan barang bukti atau informasi khusus ini merupakan jembatan yang digunakan untuk mengantisipasi perkembangan masyarakat, sehingga dengan demikian hukum tidak ketinggalan.

4.4.2 Pembuktian Tanda Tangan Elektronik

Keberadaan data elektronik dengan tanda tangan elektronik tentunya tidak releven lagi untuk diletakan atau dimasukan kedalam barang bukti atau informasi khusus, seperti rekaman *kaset, fotografi* dan sejenisnya yang sangat rentan dengan manipulasi. Padahal dengan teknologi tanda tangan elektronik, kerahasiaan, keutuhan, keotentikan dan ketidak tersangkalan suatu transaksi elektronik dapat dijamin dengan baik.

Berkaitan dengan itu, sudah saatnya posisi data atau informasi yang memanfaatkan teknologi tanda tangan elektronik “dinaikkan” kedudukannya atau paling tidak data elektronik tersebut memperoleh jaminan berupa penetapan oleh pengadilan, yang akan terus berlaku dalam setiap data atau informasi yang menggunakan tanda tangan digital.

Lagi pula, jika transaksi elektronik yang bertanda tangan telah diterima di pengadilan perdata karena dianggap sama dengan ‘surat’ maka seharusnya transaksi elektronik yang bertanda tangan juga dapat diterima langsung di pengadilan pidana.

Jika perlu semua pesan atau data elektronik yang memanfaatkan teknologi tanda tangan digital dikatagorikan sebagai bukti yang dapat berbicara sendiri (*real evidence*), dan mempunyai kekuatan pembuktian yang sempurna, mengingat tiada penyangkalan bagi pembuatnya (*non repudiation*)

4.5. Keterkaitan Acara Perdata Dan Acara Pidana

Dalam sebuah acara perdata, pembuktian keotentikan atau kesahihan sebuah transaksi elektronik diperlukan untuk menunjukan bahwa transaksi elektronik memiliki kekuatan hukum yang sama dengan alat bukti ‘tulisan’

Namun jika dalam sidang tersebut ternyata ada semacam silang pendapat terhadap keaslian atau keotentikan transaksi elektronik tersebut, artinya *mungkin* ada salah satu pihak yang melakukan kejahatan pidana komputer. Jika diduga terjadi kesalahan komputer maka diperlukan teknik pembuktian pidana yang akan dibahas pada sub-bab sesudahnya. Perhatikan bahwa ketidaksepakatan mengenai keotentikan suatu transaksi elektronik, tidak berarti bahwa telah terjadi kejahatan. Bisa saja terjadi kesalahan sistem yang diluar kontrol manusia, sehingga mengakibatkan ketidakotentikan transaksi elektronik tersebut. Hubungan sebaliknya juga dapat terjadi . Misalnya ada sebuah persidangan pidana yang sedang

menyidangkan kasus korupsi, dimana slah satu bagian dari modus operansdinya menggunakan cek digital. Cek digital tersebut, agar dikenal sebagai ‘tulisan’ maka harus menggunakan hukum acara perdata yang sudah diperbaharui untuk mengakui transaksi elektronik. Namun tentunya, jika kedua belah pihak kembali mempermasalahkan keaslian cek digital tersebut, maka keabsahan cek digital itu harus diperiksa menggunakan hukum acara pidana komputer.

BAB V
PEMBUATAN AKTA OTENTIK

5.1 Konsep Akta Otentik

Mengacu pada pasal 1868 KUHPerdata (BW), dalam transaksi elektronik dengan menggunakan tanda tangan digital, apakah dokumen yang dihasilkan dapat dinyatakan sebagai akta otentik, Bila kita mengacu pada persyaratan suatu dokumen dikatakan otentik, maka dokumen tersebut harus dibuat;

a. oleh pejabat yang berwenang
b. dihadapan pejabat yang berwenang
c. ditentukan oleh Undang-undang.

Mengutip pendapat dari Maritiman Prodjohamidjojo[40] , notaris, juru sita, PPAT, pendaftaran penduduk, adalah contoh dari pejabat umum yang berwenang. Alasan mengapa dokumen dibuat dihadapan pejabat yang berwenang adalah untuk menjadikan dokumen yang dibuat memiliki kekuatan pembuktian didepan pengadilan. Berkaitan denga hal itu maka tugas dan tanggungjawab dari notaris adalah untuk membuat akta otentik . perlu dicatat bahwa jika tidak ditentukan oleh Undang-undang, maka notaris ada pejabat umum yang dimaksud. Dalam tulisan ini, proses notarisasi merupakan cara untuk membuat akta otentik.

Pada penelitian pertama ini, kami mencoba membahas mengenai peranan dari notaris. Dalam membuat akta otentik, notaris mempunyai wewenang dalam [41];

a. penandatanganan dokumen (tidak semua notaris menandatangani akta tanah, karena ada PPAT yang mempunyai kewenangan untuk membuatnya)
b. maksud atau tujuan dokumen itu ditandatangani
c tempat dimana dokumen tiu ditandatangani

[40] *M.Prodjohamidjojo, sistem Pembuktian dan Alat-alat Bukti (jakarta, Ghalia Indonesia:1983)hal 25-26*

d waktu penandatanganan dokumen.

Persyaratan lainnya juga harus dipenuhi dalam penandatanganan

a. isi dokumen harus diketahui
b. identitas penandatanganan harus jelas
c. tempat dimana dokumen tersebut juga harus jelas
d. harus diketahui kapan dokumen tersebut ditandatangani.

5.2 Pengesahan Transaksi Elektronik

Sekarang kita lihat bagaimana peranan notaris didalam transaksi elektronik bertandatangan elektronik. Kami mengajukan suatu pendapat bahwa jika sebuah CA mendapatkan *lisensi* dari pemerintah, maka CA tersebut dapat bertindak sebagai pejabat umum. Topik mengenai skim lisensi CA akan dibahas pada sub-bab 7.4

Jika kita asumsikan bahwa pejabat umum disini mempunyai tanggung jawab yang sama dengan notaris, maka kita dapat membandingkan CA berlisensi dengan notarus. Menurut kami, CA :

a. bisa tidak mengetahui isi dari transaksi elektronik yang telah ditandatangani (karena penandatanganan dapat dilakukan secara off-line)
b. mengetahui identitas dari penandatanganan, karena pada prakteknnya setiap orang dapat melakukan pengecekan identitas penandatangan dengan certificat digital yang telah diumumkan.
c. Tidak mengetahui dimana transaksi elektronik itu ditandatangani.
d. Dapat mengetahui kapan transaksi elektronik itu ditandatangani, dengan menggunakan catatan waktu (time stamping), yang merupakkan fasilitas dari PKI.

Namun demikian alasan tersebut belumlah cukup, dalam penelitian ini kemungkinan untuk menggunakan CA berlisensi sebagai pejabat yang berwenang. Memanfaatkan infrastruktur yang diberikan CA (khususnya point b dan d), maka transaksi elektronik yang ditandatangani dapat

[41] *GHS. Lumban Tobing, Peraturan Jabatan Notaris, Cetakan ke 5 (Jakarta, Erlangga:1983, 1999) hal 49.*

dipersamakan dengan akta otentik yang dibuat di depan pejabat yang berwenang.

Jika tempat penandatanganan tidak ditentukan dikarenakan masalah geografis, ataupun pilihan hukum tidak ditetapkan di dalam perjanjian di dalam transaksi elektronik tersebut, maka teori tentang juridikasi dapat diterapkan unutk menyelesaikannya. Karena itu tidak ada masalah pada poin c.

Suatu transaksi elektronik harus ditolak oleh notaris jika dalam pembuatan atau penandatanganannya ternyata transaksi elektronik tersebut bertentangan dengan hukum (besifat melawan hukum). Tetapi jika dalam penadatanganan transaksi elektronik tersebut CA tidak hadir, dengan berdasarkan pada pasal 1320 KUHPer (BW), transaksi dinyatakan dapat dibatalkan bila transaksi tersebut ternyata melawan hukum.

Masih ada masalah lainnya yang berkaitan dengan kewenangan CA berlisensi. Kami masih mempelajari tentang transaksi elektronik yang dengan menggunakan PKI, dalam hal ini adalah CA yang berlisensi dan dapat dimanfaatkan oleh masyarakat . Padahal kita ketahui bersama bahwa notaris adalah pejabat yang berwenang, sedangkan yang lainnya tidak dapat menjadi pejabat yang berwenang, kecuali jika ditetapkan undang-undang.

Satu hal khusus yang berkaitan dengan akta otentik yang dibuat oleh CA, contohnya seperti pembuatan sertifikat tanah, tanda tangan harus dibuat oleh CA yang berlisensi, dan PPAT dapat melakukan pengecekan penandatanganan , penyimpanan sertifikat tanah tersebut.

Bab 6
Analisa Hak & Kewajiban
Subyek Hukum dalam
Infrastruktur Kunci Publik

Saat seseorang melakukan interaksi dengan seseorang dalam suatu hubungan transaksi bisnis atau tukar menukar informasi, maka akibat dari hubungan tersebut adalah timbulnya hak dan kewajiban. Di dalam terminologi hukum nasional Indonesia, seseorang yang mampu berbuat tindakan hukum dinamakan subyek hukum.

Didalam transaksi di Internet, keberadaan perlunya hukum tidak jauh berbeda dengan transaksi yang tidak dilakukan di internet. Dimana hukum tetap diperlukan untuk melindungi agar salah satu pihak tidak lalai dalam melakukan kewajibannya (wanprestasi). Jika salah satu pihak melakukan sesuatu yang tidak disepakati dalam perjanjian, maka pihak yang dirugikan dapat melakukan suatu tindakan hukum untuk menggugat pihak yang lalai dengan berlindung dibawah peraturan perundang-undangan yang berlaku.

Di Indonesia, hubungan antara dua pihak atau lebih yang sepakat untuk mengakibatkan dirinya sudah mendapatkan perlindungan hukum, dimana hal tersebut diatur di dalam kitab undang-undang Hukum Perdata (KUHPer) atau *Burgerlijk Wetboek* (BW). D dalam KUHPer, mengenai perikatan lebih speseifik lagi diatur di dalam dbuku Ke-tiga tentang Perikatan.

Dalam bab ini dijelaskan hubungan hukum antara subyek-subyek yang terdapat di dalam *public key infrastructure*, yang penerapannya dan perkembangannya disesuaikan dengan hukum nasional Indonesia yang kini berlaku.

Inti dari *Publik Kej Infrastructure* (PKI) adalah kepercayaan atau *trust*. Dimana terbentuk suatu jaringan kepercayaan antara pengguna jasa dengan pemberi jasa, dimana dalam hal ini adalah kepercayaan pengguna jasa terhadap sistem sekuritas yang ditawarkan oleh pemberi jasa.

Pertannyaan terbesar adalah bagaimana caranya menyelesaikan persengketaan jika hal tersebut terjadi. Hal ini dapat dikategorikan menjadi dua ruang lingkup :

1. Persengketaan yang terjadi anatara pengguna jasa *(subscriber)* dengan pemberi jasa *(certification authority)*.
2. Persengketaan yang terjadi antara pemberi jasa dengan pihak ketiga *(relying parties).*

Karena pihak ketiga merupakan bagian penting dari PKI, walaupun pihak ketiga pada umumnya tidak terlibat dan tidak disebutkan dalam perjanjian antara *subscriber* dengan *certification autbority*, merupakan permasalahan besar mengenai hubungan hukum antara *certification outbority* dengan *relying parties*.

Mengingat bahwa belum ada pengaturan khusus mengenai *E-Commerce* secara umum, maka akibatnya adalah bentuk hubungan antara subyek hukum di dalam PKI tunduk pada peraturan perundangan yang berlaku sekarang ini, yaitu mengenai perikatan diatur di dalam Kitab Undang-Undang Hukum Perdata, khususnya Buku Ketiga KUHPer tentang Perikatan.

6.1 Konsep Subyek Hukum.

Berdasarkan hukum nasional Indonesia dikenal subyek hukum yang dapat dikategorikan menjadi dua [42] :

1. Pribadi Kodrati.
2. Bahan Hukum *(Legal Entity).*

[42] *Dedi Soemardi S.H, Pengantar Ilmu Hukum*

6.1.1 Pribadi Kodrati.

Adalah setiap orang yang cakap menurut hukum. Cakap tidaknya seseoarang diatur di dalam pasal 1329-1330 KUHPer. Pengaturan Pribadi Kodrati sebagai subyek hukum diatur (tunduk) di dalam Kitab Undang-undang Hukum Perdata, khususnya Buku I tentang orang.

Orang yang dapat melakukan tindakan hukum sebagai subyek hukum menurut KUHPer adalah orang yang cakap, yang berarti mampu dan sadar untuk melakukan suatu tindakan hukum.

Pasal 1329 KUHPer:

> *"Setiap oarang adalah cakap untuk membuat perikatan-perikatan, jika ia oleh undang-undang tidak dinayatakan tak cakap".*

Pasal 1330 KUHPer:

> *" Tak cakap untuk memebuat suatu perjanjian adalah :*
>
> 1. *orang-orang yang belum dewasa.*
> 2. *mereka yang diatur di bawah pengampuan.*
> 3. *orang-orang perempuan" (dihapus berdasarkan Surat Keputusan Mahkamah Agung).*

Adalah sangat sulit untuk menetukan apakah seseorang adalah cakap di *cyberspace*, karena memang tidak ada paksaaan untuk memiliki indentitas resmi di Internet (tidak seperti KTP atau Paspor).

6.1.2 Badan Hukum *(Legal Entity)*

Adalah suatu badan yang diatur menurut undang-undang. Badan hukum yang dimaksudkan tersebut adalah badan hukum yang berkedudukan hukum di Indonesia dan tunduk pada hukum yang berlaku di Indonesia.

Pengaturan badan hukum sebagai subyek hukum diatur (tunduk) di dalam Kitab Undang-Undang Hukum Dagang (KUHD). Berlaku pula Undang-Undang nomor 10 tahun 1995 tentang Perseroan Terbatas (UUPT).

Berdasarkan pengkategorian diatas, maka akan timbul perbedaaan keberlakuan hukum antar subyek hukum sebagai pribadai kodrati dengan subyek hukum sebagai badan hukum yang tunduk pada KUHPer, KUHD, UUPT, UU Pasal Modal, UU Penanaman Modal Asing dan peraturan perundang-undangan lainnya yeng berhubungan dengan badan hukum.

6.2 Terjadinya Hubungan Hukum.

Sebelum membahas mengenai hak-hak dan kewajiban antara subyek-subyek hukum di dalam PKI yang mengikatkan diri merek dalam suatu perikatan, serta akibat-akibatnya, sebaiknya perlu dijelaskan terlebih dahulu mengenai dasar hukum bagi hubungan antara subyek-subyek hukum itu sendiri.

Ada dua cara bagaimana subyek-subyek hukum PKI bisa saling mengikatkan dirinya :

a. dengan membuat perjanjian/ kontrak.
b. Mengikuti hukum dan kebiasaan yang berlaku

6.2.1 Hubungan Dengan Perjanjian/ Kontrak

Menurut Kitab Undang-undang Hukum Perdata (KUHPer), hak dan kewajiban muncul setelah adanya perjanjian anatar dua pihak atau lebih, dimana akibat dari perjanjian tersebut, para pihak tersebut mengikatkan dirinya (perikatan/ *verbintenis*)[43] .

Hukum perjanjian di Indonesia menganut sistem terbuka, artinya hukum perjanjian memberikan kebebasan yang seluas-luasnya kepada masyarakat untuk mengadakan perjanjian yang berisi apa saja, asalkan tidak melanggar ketertiban umum dan kesusilaan. [44]

Dasar hukum keberlakuan kontrak atau perjanjian antara para pihak dan sistem terbuka adalah pasal 1338 ayat (1) KUHPer:

[43] *Prof. Subekti S.H., Hukum Perjanjian. Cet 12 (Jakarta, PT. Intermasa: 1990) Hal 1*
[44] *Ibid; hal 13*.

"Semua perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya".

Dengan keberlakuan pasal ini memberikan dasar dan kekuatan hukum bagi para untuk membuat perjanjian atau kontrak (asas kebebasan berkontrak), jika tidak diatur lebih khusus di dalam UU dan tidak bertentangan dengan peraturan perundang-undangan yang berlaku, khususnya mengenai syarat sahnya perjanjian yang diatur di dalam pasal 1320 KUHPer:

" Untuk sahnya suatu perjanjian diperlukan empat syarat:

1. *sepakat mereka yang mengikatkan dirinya;*
2. *kecakapan untuk membuat suatu perikatan;*
3. *suatu hal tertentu;*
4. *suatu sebab yang halal."*

Pasal-pasal dari hukum Perjanjian merupakan hukum pelengkap *(optional law),* yang berarti bahwa pasal-pasal tersebut boleh disingkirkan manakala dikehendaki oleh pihak-pihak yang membuat suatu perjanjian. Merek oleh UU diperbolehkan membuat ketentuan-ketentuan sendiri yang menyimpang dari pasal Hukum Perjanjian. [45]

Sehingga timbul suatu persengketaan, maka jika tidak diatur lebih mendetail di dalam perjanjian yang dibuat para pihak yang mengikatkan dirinya, maka akan menggunakan atau mengacu pada UU (dalam hal ini adalah KUHPer untuk masalah perjanjian misalnya).

Kontrak atau perjanjian on-line yang ada sekarang ini bentuknya sebagian besar adalah kontrak atau perjanjian yang dibuat secara sepihak, yaitu oleh pihak yang menawarkan barang atau jasa. Sehingga jika pihak *subscriber* ingin membeli atau menggunakan barang atau jasa yang diberikan oleh pihak penawar, maka akan harus menyepakati kontrak yang telah dibuat terlebih dahului.

[45] *Ibid*

Permasalahan yang muncul adalah apabila jika timbul persengketaan dimana di dalam perjanjian tidak diatur, dan di dalam KUHPer tidak diatur secara jelas. Sehingga adalah sangat penting dan dengan jelas menetapkan secara mendetail mengenai batas-batas dari hak dan tanggung jawab di dalam suatu perjanjian.

Selama belum ada UU yang mengatur secara mendetail mengenai batasan-batasan maka hak dan kewajiban dari pihak-pihak daam PKI sangat tergantung dan bersumber pada asas kebebasan berkontrak yang dituangkan dalam pasal 1338 KUHPer. Jika perjanjian tersebut tidak mengatur mengenai persengketaan yang mungkin akan terjadi secara mendetail dan jelas, maka akibatnya akan tunduk pada KUHPerdata (dan peraturan perundang-undangan lain yang berlaku) dengan segala konsekuensinya.

6.2.2 **Mengikuti Hukum dan Kebiasaan dalam Perjanjian**.

Walaupun belum adanya suatu bentuk perundangan khusus mengatur mengenai hubungan subyek hukum yang terlibat di dalam PKI, pembuat KUHPer telah memberikan keleluasan untuk para pembuat perjanjian dalam bentuk suatu kebiasaaan. Hal ini diatur dalam Bagian Keempat Buku III Kitab Undang-undang Hukum Perdata tentang penafsiran suatu perjanjian.

Melihat bahwa sifat dari transasi *on-line* adalah perjanjian sepihak yang dibuat oleh salah satu pihak; dalam halnya PKI maka pihak yang membuat perjanjian (kontrak) tersebut adalah CA (*Certification\ Autbority).*

Bahwa hak dan kewajiban dari CA dengan pihak-pihak yang berhubungan dengannya *(subscriber)* yang dituangkan perjanjian *on-line* tersebut, dan sudah umum digunakan oleh pengguna internet di cyberspace, maka sudah tercipta suatu kebiasaaan dalam perjanjian yang digunakan oleh subyek hukum dalam PKI.

Dasar hukum untuk kebiasaaan terlihat jelas dalam pasal-pasal berikut :

Pasal 1339 KUHPer:

> *"Suatu perjanjian tidak hanya mengikat untuk hal-hal yang dengan tegas dinyatakan di dalamnya, tetapi juga untuk segala sesuatu yang menurut sifat perjanjian ,diharuskan oleh kepatutan, kebiasaan atau undang-undang"*

pasal 1346 KUHPer:

> *"Apa yang meragu-ragukan harus ditafsirkan menurut apa yang menjadi kebiasaan dalam negeri atau tempat, dimana perjanjian telah dibuat "*

pasal 1347 KUHPer :

> *"Hal-hal yang, menurut kebiasaan selamanya diperjanjikan, dianggap secara diam-diam dimasukan dalam perjanjian, meskipun tidak dengan tegas dinyatakan "*

pasal 1339 KUHPer memberikan landasan pertama mengenai pengakuan dan perlindungan hukum terhadap kebiasaan yang sudah tercipta dalam perjanjian.

Pasal 1346 KUHPer memberikan keleluasaan lebih dimana suatu perjanjian mengikuti standar kebiasan dalam negeri atau di tempat perjanjian telah di buat (jika meragukan isinya), sehingga secara yuridis, walapun tidak jelas ditekankan pengaturan mengenai tata cara pelaksanaan, jika hal tersebut sudah diakui sebagai suatu kebiasan dalam perjanjian di PKI, maka kebiasan tersebut mendapatkan pengakuan yuridis.

Hal mengenai kebiasaan ini lebih diperkuat di pasal berikutnya (pasal 1347) dengan menegaskan bahwa suatu kebiasan dianggap secara diam-diam dimasukan dalam perjanjian, walaupun tidak jelas dinyatakan.
Permasalahan yang timbul akibat dari pasal–pasal ini, adalah apakah konvensi yang berlaku secara umum dalam penggunaan teknologi informasi

berbasis PKI yang menebus batas antar negara juga termasuk dalam batasan, *kebiasaan*, seperti tercantum dalam pasal 1347 Kemudian apa yang terjadi jika ada beberapa konvensi pilihan ? Mana yang dipergunakan ?
Berdasarkan hal tersebut, maka kami menganjurkan agar perjanjian antara CA dengan *subscriber* (atau dengan pihak– pihak lainya) harus dibuat secara detail agar ada kejelasan.
Perlu diingat bahwa jika sudah diatur lebih jelas didalam perjanjian, maka klausa-klausa didalam perjanjian tersebut akan membatalkan unsur kebiasaan dalam perjanjian , karena asas terbuka yang dianut dalam perjanjian.
Jika suatu perundangan yang mengenai PKI telah disahkan, dan peraturan tersebut cukup detail dalam mengatur hubungan antar subyek, maka dalam perjanjian antara CA dengan *subscriber* (atau kemukinan juga dengan *relying party*) tidak perlu mengatur hal-hal yang sudah diatur dalam perundangan.

6.3 Hak dan Kewajiban Subyek-Subyek Hukum Dalam PKI

Sekarang akan dijelaskan lebih spesifik mengenai hak-hak dan kewajiban subyek hukum dalam PKI, yang dibuat bedasarkan kebiasaan yang sudah ada di dalam PKI dan juga dengan penelitian perbandingan dengan undang-undang *digital signature* yang sudah berlaku di negara lain(seperti Utah *Digital Signature Act 1996*), disesuaikan keberlakuanya dengan hukum nasional yang kini berlaku .

6.3.1 *Subscriber* (pengguna jasa)

Pihak *subscriber* menggunakan jasa yang ditawarkan oleh CA untuk mengamankan transaksinya yang dilakukan secara on-line. *Subscriber* dalam prateknya dapat berhubungan dengan pihak ketiga atau *relying parties*, yang secara tidak langsung juga berhubungan dengan CA.
Subscriber dapat dikatagorikan sebagai pribadi kodrati dan dapat juga sebagai badan hukum.

6.3.1.1 **Kewajiban-kewajiban** :

1. Menyepakati segala isi dari *Cartification Statement* (CPS) sebagai perjanjian/ kontrak antara pengguna jasa *(subscriber)* dengan pemberi jasa (CA).
2. Memberikan keterangan sebenarnya dan menjamin bahwa segala informasi yang diberikan untuk proses pensertifikasian dan keperluan administrasi dari CA, RA dan pihak-pihak lain untuk berkepentingan dengan proses pensertifikasian adalah benar dan sah.

Penipuan; Pasal 1328 ayat(1) KUHPer:

> *"Penipuan merupakan suatu alasan untuk pembatalan perjanjian, apa bila tipu muslihat, yang di pakai oleh salah satu pihak, adalah sedemikian rupa hingga terang dan nyata bahwa pihak yang lain tidak telah membuat perikatan itu jika tidak dilakukan tipu-muslihat tersebut"*

Pasal 1335 KUHPer:

> *"Suatu perjanjian tanpa sebab, atau yang telah dibuat karena sesuatu sebab yang palsu atau terlarang, tidak mempunyai kekuatan"*

Jika ternyata *subscriber* memberikan identitas palsu atau tidak sebenarnya, dimana di perlukan untuk keperluan keamanan, maka hal tersebut dapat dijadikan dasar untuk batal demi hukum bagi perjanjian antara *subscriber* dengan CA atau RA.

3. Segera melaporkan kepada RA atau kepada CA jika diketahuinya adanya kebobolan, penyalahgunaan, kerusakan terhadap kunci privat.

4. *Subscriber* diwajibkan untuk melindungi kunci privatnya, dan apabila ia mengetahui kunci privat trsebut telah disalahgunakan atau telah dirusak. Saat seorang *subscriber* telah membuat atau menerima kunci publik atau

kunci privatnya[46], adalah sangat penting agar ia merahasiakan kunci privatnya dari publik (umum), karena jika orang lain mendapatkan akses terhadap kunci privatnya, maka kunci tersebut dapat di-duplikat, untuk membuat tanda-tangan digital sehingga dapat terjadi penggunaan illegal[47].

5. Tidak dengan sengaja memberikan kunci privatnya kepada orang lain, kecuali telah disepakati sebelumnya didalam CPS ataupun perjanjian lanjutan dengan CA.

6. Mengambil upaya-upaya yang perlukan untuk memastikan keamanan kunci publik agar tidak dibobol atau jatuh ke tangan pihak yang tidak berkepentingan.

7. Tidak menggunakan kunci privatnya untuk tindakan-tindakan yang menurut peraturan perundang-undang nasional Indonesia bertentangan atau dianggap sebagai tindakan kriminal.

Pasal 1254 KUHPer

> *"Semua syarat yang bertujuan melakukan sesuatu yang tak mungkin terlaksana, sesuatu yang bertentangan dengan kesusilaan baik, atau sesuatu yang dilarang oleh undang-undang adalah batal dan berakibat bahwa perjanjian yang diantungkan padanya, tak berdaya".*

6.3.1.2 Hak-hak:

1. menggunakan kunci privatnya untuk keperluannya yang tidak bertentangan dengan CPS atau peraturan perundang-undangan nasional Indonesia bertentangan atau dianggap sebagai tindakan kriminal.

---

[46] *Walaupun di dalam praktek umum, kunci privat biasanya dibuat oleh CA, dalam perkembangannya jika jasa CA mengizinkan, maka kunci privat yang bersifat sangat rahasia, biasa juga dibuat oleh CA.*

[47] *John Angel,Why use Digital for Electronic Commerce?", (United Kindom: Journal of Information law and Technology, 1999), hal 3 http://www.lammarsik.ac.uk/jill/99-2/angel.htm/*

Pasal 1254 KUHPer

> *“Semua syarat yang bertujuan melakukan sesuatu yang tak mungkin terlaksana, sesuatu yang bertentangan dengan kesusilaan baik, atau sesuatu yang dilarang oleh undang-undang, adalah batal dan berakibat bahwa perjanjian yang diantungkan padanya, tak berdaya".*

2. Meminta atau mengajukan permohonan pencabutan sertifikat kepada CA atau RA diketahuinya adanya kebobolan, penyalagunaan, kerusakan terhadap kunci privat.

3. Menunjuk wakil atau penerima kuasa untuk mengatasnamakan dirinya untuk menguasai atau memegang kunci privat.

6.3.2. *Certification Authority* (CA)

Pihak Certification Authority (CA) memberikan jasa keamanan kepada *subscriber*, dimana CA dapat berperan sebagai badan hukum, ataupun sebagai pribadi kodrati (misalnya Pretty Good Privacy/ PGP).

Merujuk pada pasal 1338 KUHPer, maka perjanjian antara CA dan *subscriber* mengikat mereka seperti undang-undang. Dalam PKI, perjanjian antara CA dengan *subscriber* dinamakan *Certification Practise Statement* (CPS), yang merupakan perjanjian ”sepihak”, artinya yang dibuat oleh satu pihak, dalam hal ini adalah CA. Sehingga jika *subscriber* sepakat atas ketentuan-ketentuan (klausa-klausa) yang dicantumkan di dalam perjanjian yang dibuat oleh CA tersebut (CPS), maka perjanjian tersebut akan mempunyai kekuatan hukum, walaupun tidak dibuat bersama-sama, hal ini berdasarkan pasal 1320 KUHper, butir (1) mengenai kata adanya kata sepakat antara para pihak untuk mengikatkan dirinya.

6.3.2.1 *Implikasi Hukum Lisensi Terhadap* CA

Di negara-negara yang sudah mempunyai undang-undang *Digital Signatura* atau undang-undang yang mengakui keberadaan CA terdapat perbedaan

kategori terhadap CA, dalam arti CA yang mendapatkan izin pratek dari pemerintah. Izin pratek ini mengindikasikan bahwa CA tesebut sudah memenuhi standar dari pemerintah yang diperuntuhkan sebagai standar minimal untuk melindung para pengguna jasa dari CA.

Perlu diingat bahwa CA dapat melakukan fungsinya/berpraktek tanpa mendapatkan lisensi dari pemerintah negara tersebut, tetapi pemerintah tidak memberikan jaminan perlindungan penuh secara hukum terhadap persengketaan yang mungkin terjadi jika warga negaranya melakukan hubungan dengan CA yang tidak berlisensi tersebut. Contoh, jika terdapat persengketaan terhadap CA yang tidak berlisensi karena adanya kebobolan terhadap sistem keamanannya, maka di pengadilan sistem keamanannya perlu dibuktikan lagi dengan mengunakan saksi-saksi ahli dsb, karena tidak diakui/mengikuti oleh standar pemerintah, dimana jika Ca tersebut berlisensi hal tersebut tidak perlu dibuktikan lagi. Penjelasan detail mengenai skim lisensi dapat dibaca pada bab Bab 7.
Pemerintah dalam hal ini perannya dipegang oleh badan pengawas (*controller).*

6.3.2.2. Kewajiban-kewajiban

1. Berkedudukan di dalam wilayah teritorial Republik Indonesia atau mempunyai representasi di dalam wilayah teritorial Republik Indonesia.

2. Membuktikan kepada Badan pengawas modal finansial yang cukup untuk menjalankan fungsi sebagai CA.

3. Menggunakan pegawai yang berpengalaman dalam proses pensertifikasian dan tidak mempunyai latar belakang kriminal, terutama yang berhubungan dengan penipuan.

4. Membuat *Certification Practise Statement* (CPS) untuk kepentingan calon pengguna jasa *(prospective subscriber),* sebagai perjanjian/ kontrak antara pengguna jasa *(subscriber)* dengan pemberi jasa (CA).

5. Mematui segala peraturan perundang-undangan yang berlaku, yang berhubungan dengan eksistensinya sebagai CA.

6. (Jika berlisensi) mematuhi segala keputusan yang dikeluarkan oleh Badan Pengawas, baik berupa perintah atupun regulasi yang dibuat oleh Badan Pengawas.

7. Menggunaan sistem yang terpercaya dan menggunakan standar yang lazim diterima dalam kebiasaan PKI (atau menggunakan standar Badan Pengawas jika berlisensi) dalam proses pensertifikasian .

8. Mencabut atau membekukan sementara sertifikat Digital jika diminta oleh *subscriber* yang namanya tertera di dalam sertifikat Digital tersebut .

9. Memberikan pemberitahuan kepada *subscriber* yang akan dipublkasikan di dalam *Certificate Revocation List* (CRL) jika bermaksud untuk mencabut atau membekukan untuk sementara atau untuk jangka waktu tidak tertentu sertifikat digital atas inisiatif CA itu sendiri karena alasan-alasan tertentu (penjelasan alasan- alasan tersebut terdapat di dalam Hak dari CA).

10. Melaporkan segala bentuk enkripsi atau penyandian kepada Badan Pengawas dan / atau Lembaga Sandi Negara atas dasar keamanan nasional. Apakah dilaporkan kepada Badan Pengawasan dan / atau lembaga Sandi Negara tergantung pengaturan UU lebih lanjut.

6.3.2.3 Hak-Hak

1. Mencabut (atau membekukan untuk waktu tertentu atau tidak tertentu) Sertifikat Digital karena alasan-alasan yang termasuk tetapi tidak terbatas pada:

    a. Mencabut Sertifikat Digital karena telah daluarsa (jangka waktu keberlakuan sertifikat Digital telah habis).

b. Terdapat kebocoran atau kebobolan terhadap informasi ataupun sistem yang mengakibatkan Sertifikat Digital tersebut tidak lagi aman (setelah memberikan pemberitahuan kepada *subscriber* yang namanya tertera di dalam Sertifikat Digital).

c. Mencabut Sertifikat Digital jika subsriber yang namanya tertera di dalam Sertifikat Digital setelah menerima bukti berupa salinan surat kematian *subscriber* tersebut atau bukti-bukti lainya yang cukup dan sah untuk mendukung hal tersebut.

2. Menggunakan sistem yang terpecaya untuk keperluan enkripsi dan proses pensertifikasian.

6.3.3 *Relying party* (pihak ketiga)

Pihak ketiga di dalam PKI memegang peranan yang sangat penting, sehingga diperlukan kejelasan hukum mengenai perlindungan dan penyelesaian persengketaan bagi pihak ketiga. Permasalahan timbul karena secara perdata nasional, perjanjian hanya berlaku bagi para pihak yang membuatnya, sehingga hal ini menimbulkan pertanyaan bagi perlindungan dan penyelesaian persengketaan bagi pihak ketiga, dimana inti permasalahannya adalah hubungan antara CA dengan pihak ketiga tersebut, yang mungkin tidak dicantumkan didalam perjanjian antara *subscriber* dengan pihak ketiga. Sehingga jika terjadi hal-hal yang tidak diinginkan yang mengakibatkan kerugian di pihak ketiga, yang timbul dari pihak CA, maka CA bisa saja menurut hukum yang berlaku lepas tangan, kecuali jika diatur lain dalam peraturan perundang-undangan yang berlaku.

Berdasarkan hukum nasional (KUHPer), keberadaan *relying party* dalam PKI adalah sangat unik karena berdasarkan dasar perjanjian, maka perjanjian hanya mengikat pihak-pihak yang mengikatkan dirinya. Hal ini disebutkan dalam pasal 1338 ayat (1) dan pasal 1340 ayat (1) KUHPer:

Pasal 1338 ayat (1) KUHPer:

> *"Semua perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya".*

Pasal 1340 ayat (1) KUHPer:

> *"Suatu perjanjian hanya berlaku antara pihak-pihak yang membuatnya".*

Hal ini menimbulkan pertanyaan mengenai bagaimana perlindungan hukum terhadap pihak ketiga yang berkepentingan dengan *subscriber* yang secara tidak langsung juga berkepentingan terhadap keamanan/ sekuritas yang digunakan oleh *subscriber* tersebut yang diberikan oleh CA.

Menurut hukum nasional hal ini bisa diselesaikan dengan 2 cara:

1. Menyerahkan kepada aturan yang sudah berlaku berlandaskan hukum yang sudah ada.

2. Mengatur dan mengakui perlindungan kepada *relying parties* oleh CA dalam CPS (yang dibuat juga oleh CA).

6.3.3.1 Pengaturan berlandaskan hukum yang sudah ada saja

Sebenarnya sebuah perjanjian hanya berlaku diantara pihak-pihak yang membuatnya, dan tidak boleh merugikan pihak ketiga. Pasal yang berhubungan dengan poihak ketiga misalnya pasalanya 1340 KUHPer.

> *"Suatu perjanjian hanya berlaku antara pihak-pihak yang membuatnya. Suatu perjanjian tidak dapat membawa rugi kepada pihak-pihak ketiga ……"*

Pasal ini berarti suatu perjanjian tidak dapat mengakibatkan atau berakibat suatu kerugian bagi pihak ketiga.
Dalam KUHPer terdapat beberapa pasal yang dapat melindungi kepentingan pihak ketiga walaupun belum ada perjanjiannya:

Pasal 1365 KUHPer:

> *"Tiap perbuatan melanggar hukum, yang membawa kerugian kepada seorang lain, mewajibkan orang yang yang karena salahnya menerbitkan kerugian itu, menggantikan kerugian tersebut".*

Jika konteks kerugian diakibatkan oleh suatu perbuatan melanggar hukum, dimana hal tersebut misalnya terjadi dari pihak CA (misalnya karena ulah salah seorang pegawainya), maka berdasarkan pasal ini CA secara hukum berkewajiban untuk menggantikannya secara penuh.

Pasal 1366 KUHPer:

> *"Setiap orang bertanggung jawab tidak saja untuk kerugian yang disebabkan perbuatannya, tetapi juga untuk kerugian yang disebabkan kelalaian atau kurang hati-hatinya".*

Pasal ini memberikan perlindungan hukum kepada *relying parties* untuk konteks tindakan kelalaian dari pihak CA dalam melaksanakan fungsinya sebagai pemberi jasa pelayanan. Dengan keberadaan pasal ini, pihak ketiga dapat menuntut ganti rugi, walaupun tidak diperjanjikan sebelumnya.

Pasal 1367 KUHPer:

> *"Setiap orang bertanggung jawab tidak saja untuk kerugian yang disebabkan perbuatannya sendiri, tetapi untuk kerugian yang disebabkan perbuatan orang-orang yang menjadi tanggungjannya atau disebabkan oleh barang-barang yang berada di bawah pengawasannya".*

Pasalnya ini memperkuat kedua pasal sebelumnya dengan memperluas ruang lingkup pribadi kodratinya dan obyeknya, yang menjadi tanggung jawab dari padanya, dimana dalam hal ini dapat berupa kelalaian pegawai-pegawai dari CA dan dalam konteks ini bisa juga meliputi sistem keamanan CA sebagai objek. Pasal ini dalam KUHPer juga memberikan dasar hukum yang sangat kuat bagi keberadaan teknologi informasi, karena yang menjadi objek adalah sistemnya.

Kegagalan Sistem. Jika tidak ada klausul dalam CPS yang mengatur kewajiban CA jika terjadi kegagalan sistem (dengan kata lain gagal menyediakan s*ervices* yang dijanjikan), maka sebenarnya berdasarkan pasal 1245 KUHPer CA bisa tidak memberikan ganti rugi kepada *relying party*, asalkan disebabkan oleh hal-hal yang tidak disengaja dan memaksa. Agar tidak terjadi 'penyalahgunaan' oleh CA ('lari dari tanggung jawab'), ada beberapa hal yang perlu diperhatikan :

1. Frase 'tak disengaja dan memaksa' dalam pasal 1245 tersebut, harus ditafsirkan sebagai *force majeur* atau bencana pasar.

2. Jika ada peraturan baru mengenai tanda tangan elektronik dan CA, harus diatur prinsip-prinsip umum menganai ganti rugi yang diberikan CA kepada *relying party*.

3. CPS yang dibuat oleh CA harus detail untuk meliputi hal-hal yang berkenaan dengan kegagalan sistem CA untuk memberikan pelayanan (lihat sub-bab berikutnya).

6.3.3.2 Pengaturan mengenai relying party dalam CPS yang dibuat CA.

Secara umum hal ini kelihatannya tidak bermasalah, tetapi dari menurut hukum perdata sebagaimana hal yang disebutkan diatas dalam pasal 1338 dan 1340 KUHPer, perjanjian tersebut hanya berlaku bagi para pembuat perjanjian tersebut.

Untuk memasukan *relying party* ke dalam perjanjian, dapat dilakukan dengan beberapa pendekatan :

1. Sepakat dengan cara menerima CPS yang dibuat CA.

Menurut Pasal 1320 ayat (1) KUHPer. Ayat (1)

"kata sepakat mereka yang mengikatkan dirinya"

Walaupun pihak *relying party* tidak ikut serta dalam pembuatan CPS (seperti juga *subscriber*), dan tidak menyepakati isi perjanjian tersebut secara langsung, namun dengan melakukan hubungan dengan pihak *subscriber* yang juga menggunakan jasa CA, secara tidak langsung (implisit) sebenarnya juga menyepakati menggunakan jasa dari CA.

Selain itu, untungnya pasal 1317 KUHPer memeperbolehkan kita untuk menyertakan pihak ketiga dalam perjanjian.

Kami merekomondasikan sebaiknya ada beberapa klausul dalam CPS tersebut yang kira-kira menyatakan kalau ada *relying party* yang menggunakan kunci publik yang dihasilkan oleh PKI CA yang menerbitkan CPS tersebut, maka *relying party* itu terikat dalam CPS tersebut. Permasalahannya sebenarnya nanti kalau terjadi dispute, dimana *relying party* harus membuktikan kepada hakim bahwa dia memang telah menggunakan kunci publik dari seorang *subscriber* CA yang bersangkutan.

2. Cara yang kedua adalah dengan membuat suatu perjanjian atau kontrak lanjutan antara subscuber dengan CA, yang secara jelas menempatkan nama-nama pihak yang akan menjadi *relying partys.* Hal ini lebih mudah (dan aman), jika sudah jelas pihak-pihak mana yang akan menjadi relying parties. Ini bermanfaat jika komunitas yang melakukan transaksi sudah teridentifikasi (dengan kata lain, *relying party*s-nya sudah teridentifikasi sebelumnya).

Walaupun praktek ini bisa dikatakan tidak lazim dalam kebiasaan dalam PKI, namun menuruit hukum nasional, hal ini jauh lebih memberikan kepastian dan perlindungan hukum terhadap relying parties, karena sudah adanya suatu bentuk perjanjian / kontrak baru, sehingga tidak perlu lagi tergantung dari pada isi pasal-pasal yang ada di dalam KUHPer.

Namun kekurangan yang ada dari cara ini adalah jika relying partis yang belum bisa diketahui identitasnya dan bertambah terus setiap saat, maka akan berakibat terhadap pembuatan kontrak-kontrak baru untuk setiap relying parties yang baru.

Praktek ini lebih digunakan jika para pihak ingin menggunakan tingkat keamanan dan perlindungan hukum yang maksimum yang bisa diberikan oleh hukum nasional kita.

6.3.4 Registrasi Authority (RA)

Sebenarnya RA dan Repository merupakan bagian dari pada CA. Namun dalam perkembangannya dan kebutuhan, keberadaan RA dapat berdiri sendiri. Dalam PKI, keberadaan RA dapat dipersamakan dengan juru daftar yang mencatat dan membuktikan keabsahan identitas calon *subscriber* yang akan menggunakan jasa dari CA.

6.3.4.1 Kewajiban-kewajiban

1. Mencatat dan mengotentifikasi identitas dari calon pelanggan (prospective *subscriber*) untuk keperluan administrasi dan proses pensertifikasian.

   Proses ontentifikasi identitas dari calon pelanggan tersebut bisa dikategorikan menjadi 3 (tiga) tingkatan[48].

   a. Otentifikasi identitas dengan menggunakan e-mail.

      Proses identifikasi semacam ini memberikan kepastian identifikasi minimal, biasanya hanya digunakan untuk memastikan keberadaan, bukan untuk memastikan apakah orang itu (identitasnya) benar-benar atau tidak.

   b. Otentifikasi identitas dengan registrasi on-line.

[48] *John Angel op cit; hal. 4*

Proses identifiksi yang umumnya digunakan di Internet, dengan memberikan bukti-bukti nama, alamat dan informasi pribadi lainnya yang diperlukan.

c. Otentifikasi identitas secara fisik

Merupakan identifikasi paling meyakinkan, jika calon *subscriber* datang sendiri ke RA. Hal ini biasa dilakukan jika diperlukan tingkat keamanan yang sangat tinggi.

Namun dalam hal otentifikasi identitas pihak CA dan khususnya pihak RA tidak boleh sembarangan dalam meregistrasi orang yang mengakui sebagai pribadi kodrati atau yang mengaku mewakili badan hukum, karena orang-orang yang dianggap tidak cakap (Pasal 1330 KUHPer), tidak dapat bertanggung jawab secara hukum.

2. Membuat kunci privat back-up yang digunakan sebagai cadangan, jika kunci privat dari *subscriber* hilang (key recovery).

6.3.5 Repositery

Sama dengan RA dalam sejarah PKI, keberadaan Repository dalam perkembangannya semula merupakan salah satu fungsi dari CA, numun dapat berdiri sendiri terpisah dari CA.

6.3.5.1 Kewajiban-kewajiban

1. menggunakan sistem yang terpercaya untuk proses penyimpanan sertifikat digital.

2. Mempunyai data base yang menggunakan sistem yang terpercaya yang:

    a. Digunakan untuk memuat sertifikat digital
    b. Memuat daftar sertifikat digital yang dibekukan atau dicabut.

6.3.5.2 Hak

1. mengajukan permintaan untuk diterima sebagai badan repository yang sah dari badan Pengawas (jika repository tersebut tidak dibawah CA / berdiri sendiri)

6.3.6 Controller (Badan Pengawas)

Istilah Controller di pinjam dari Digital Signature Act 1997 Malaysia; sedangkan di Utah (yang menelurkan undang-undang tanda tangan digital pertama), menggunakan istilah Division. Jika diterjemahkan menurut fungsinya, maka kurang lebih berarti badan pengawas. Mengingat bahwa perkembagan teknologi sangat cepat, dan ketakutan bahwa dalam hal-hal tertentu UU yang ada akan kurang memadai untuk mengikuti perkembangan tersebut, maka timbullah kebutuhan mengenai adanya suatu instansi pemerintah yang mengatur regulasi terhadap perkembangan teknologi selanjutnya, dan juga berperan sebagai tempat untuk menyelesaikan perkara atau sengketa yang mungkin dialami oleh CA.

Keberadaan Badan pengawas dalam PKI ini sebenarnya bisa dikategorikan menjadi 2:

1. Sebagai Badan Pengawas, dimana Badan Pengawas sebagai badan pemerintah terbatas fungsinya pada peran untuk mengatur dan membuat regulasi mengenai PKI (regulator)
2. Sebagai Otoritas Sertifikat Nasional (National CA), dimana dapat juga berperan selain membuat regulasi, juga dapat menerbitkan sertifikat atas nama negara.

Badan Pengawas yang akan dijelaskan dalam Hak-hak dan Kewajiban Subyek Hukum dalam PKI akan terbatas menjelaskan peran Badan pengawas pada butir (1) diatas.

Berikut ini adalah hak dan kewajiban Badan Pengawas. Konteks dari CA yang dinyatakan dibawah ini, jika tidak sebutkan kategorinya, merujuk kepada CA yang berlisensi.

6.3.6.1 Kewajiban-kewajiban

1. membuat segala regulasi yang dianggap perlu untuk menjaga kelancaran lalu lintas transaksi dalam PKI
2. Menyelesaikan dan memberikan keputusan untuk segala persengketaan yang dibawah kepadanya yang berhubungan dengan CA.

6.3.6.2 Hak-hak

1. Menerbitkan suatu lisensi ijin praktek untuk CA yang mempunyai lisensi.
2. Mencabut atau membekukan ijin lisensi dari suatu CA alasan-alasan tertentu menurut diskresinya adalah melanggar UU atau peraturan perundang-undangan yang berlaku.
3. Menyelidiki kegiatan otoritas sertifikasi yang berlisensi jika dianggap perlu atau karena adanya indikasi atau kecurigaan adanya tindakan dari CA yang melawan hukum.

6.3.6.3 Wewenang

1. Membuat regulasi untuk mengatur perubahan yang mungkinterjadi dalam PKI, yang mungkin tidak diatur di dalam peraturan perundang-undangan yang berlaku.
2. Memberikan, pencabut atau membekukan izin kerja (lisensi) Certification Authorty.
3. Membuat standar-standar untuk di pakai di PKI Indonesia:
    - Standar Sistem Enkripsi dan proses Sertifikat
    - Syarta-syarat pendirian CA
    - Standar yang digunakan untuk CPS

Bab 7
STANDAR PENGAKUAN TANDA TANGAN ELEKTRONIK & SKIM LISENSINYA

7.1 Latar Belakang

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

Artinya, seorang *relying party* bisa saja tidak mempunyai tanda tangan atau sertifikat digital seorang *subscriber* dari sebuah CA lain yang memilik CPS yang berbeda dengan CPS yang telah biasa diakui sang relying party. Dengan kata lain, dua orang yang berasal dari domain CA yang berbeda, bisa jadi saling tidak mengakui tanda tangan yang dihasilkan dari domain lainnya dengan alasan bahwa standar CPS dari kedua CA tersebut berbeda. Yang menarik adalah, bisa saja kedua CA tersebut menganggap CPS milikinya masing-masing lebih tinggi kualitasnya dibandingkan yang lain.

Sebenarnya dalam pembahasan teknis mengenai PKI, sudah dijelaskan mengenai bagaimana cara CA bisa mengakui keberadaan CA lainnya. Ini dapat dilakukan antara lain dengan cross certification, hierarchial networktree, dan lain sebagainya.
Sebenarnya ada cara non-teknis (lebih konseptual) agar tanda tangan yang berasal dari dua domain dapat diakui. Hal ini dilakukan dengan cara menetapkan suatu standar operasi minimal yang harus dipatuhi CA. Dengan memenuhi standar operasi minimal, maka sertifikat digital ataupun tanda tangan elektronik yang dihasilkan dari sebuah domain CA tertentu dapat diakui pihak manapun yang telah mengakui standar operasi minimal tersebut. Contoh spesifiknya, dalam hal mengelola sertifikat, maka CA tersebut harus tunduk pada standar CPS minimal.

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

Dalam bab ini kita tidak membicarakan secara teknis apa yang harus termaktub dalam standar minimum tersebut, melainkan lebih kearah bagaimana standar itu diakui oleh banyak pihak (termasuk oleh pemerintah). Di beberapa negara, seperti yang akan dijelaskan nanti, pemerintah memberikan lisensi kepada CA yang sudah beroperasi pada standar minimum tertentu.

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

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

7.2 Tingkat Standar Pengakuan

Menurut Baker dan Kuner[49], ada beberapa cara jenis standar pengakuan pengakuan terhadap tanda tangan elektronik yang diakui negara:

1. Mengenakan standar minimalistik (longgar).
2. Mengenakan standar ketat.
3. Penerapan beberapa standar, atau dua standar.

[49] *Stewart Baker dan Chris Kuner, An Analysis of International Electronic and Digital Signature Implementation Intiatives, (Internet Law and policy Forum, September 2000) http: / /www.ilpf.org/disig/ analysis – IEDSII.htm*

7.2.1. Standar minimalistik (Longgar)

Sebuah, tanda tangan elektronik, sebenarnya tidak berarti pasti aman. Kalau misalnya saja manejemen pengoperasian CA buruk, tingkat ke ontentikan tanda tangan elektronik yang di hasilkan menjadi rendah (dapat disangkal oleh seorang ahli sekuriti). Tetapi memang, jika dibandingkan dengan sistem kriptografi kunci simetrik yang memiliki standar manajemen operasi yang sama, sistem kriptografi kunci publik (untuk membuat tanda tangan elektronik) jauh lebih aman. Berdasarkan dalih bahwa sistem kriptografi kunci publik secara umum lebih aman ketimbang kritografi kunci simetrik dan tanda tangan konvensional (biasa), maka mungkin suatu sistem hukum suatu negara menyatakan bahwa sebuah tanda tangan digital tidak boleh ditolak di pengadilan hanya karena ada dalam bentuk elektronik (terlepas dari tiap negara itu ada standar yang diakui oleh pemerintah atau tidak). Masalah nanti di pengadilan teryata tanda tangan elektronik itu terbukti telah dipalsukan, itu adalah urusan lain (kejahatan pidana komputer) .Yang penting - minimal - tanda tangan elektronik di akui keberadaanya. Beberapa negara common law (misalnya Kanada, Irlandia, Australia, dan Amerika Serikat) mengakui tanda tangan elektronik dipengadilan, terlepas apakah sudah mengikuti standar baku tertentu atau belum. Perlu di catat bahwa tidak semua negara penganut common law menggunakan pendekatan standar minimalistik. Filipina juga menerapkan standar yang longgar.Meskipun standar untuk pengakuan tanda tangan elektronik longgar, tetap saja diperadilan harus dibuktikan bahwa tanda tangan elektronik itu terjamin keaslianya. Cara untuk membuktikan keasliannya dibahas pada sub-bab 7.3.1.

7.2.2 Penerapan Standar Ketat

Di sisi lain, ada pula pula negara-negara yang sistem peradilanya hanya menerima tanda tangan elektronik yang sudah dijamin dahulu “keamanannya “. Artinya tanda tangan elektronik yang dihasilkan oleh suatu CA tersebut harus sulit sekali dipalsukan, sehingga negara berani menjamin keotentikanya. Pada umumnya, penerapan standar ketat Ini dilakukan dengan cara mewajibkan audit terhadap CA oleh auditor yang dapat dipercaya, berkenaan dengan

standar operasi dan CPS-nya .setelah menerima hasil audit yang menyatakan bahwa sistem opersi dan CPS dari CA tersebut dianggap cukup layak dan aman, negara dapat memberikan lisensi [50] kepada CA. Tanda tangan elektronik yang di hasilkan oleh infrastruktur kunci publik CA berlisensi tersebut dapat langsung diakui pengadilan tanpa perlu dibuktikan dahulu (presumption of authenticity).

7.2.3 Penerapan Beberapa Standar atau Dua Standar.

Tetapi ada juga negara-negara yang mengakui keberadaan tanda tangan elektronik, baik yang berasal CA yang berlisensi dengan CA yang tidak berlisensi. Jadi kalau ada skema lisensi CA pun, tidak berarti bahwa semua CA wajib berlisensi.Singapura memiliki skim lisensi CA yang tidak wajib. Namun jika dibandingkan CA yang tidak berlisensi, maka CA yang berlisensi memiliki beberapa keuntungan yang tidak dimiliki CA yang tidak berlisensi. Keuntungan tersebut antara lain:

- Prinsip pembuktian terbalik atas keaslian tanda tangan elektronik di pengadilan. Tanda tangan elektronik yang dihasilkan dari PKI CA berlisensi tersebut langsung diakui dipengadilan sederajat dengan tanda tangan biasa. Jadi jika ingin dibantah, maka harus dibuktikan sebaliknya (bahwa CA tersebut melanggar standar operasi yang ditetapkan untuk mendapatkan lisensi).

- Adanya reliance limit jika CA harus memberikan ganti rugi terhadap *subscriber*nya manakala terjadi bencana / masalah.

- Adanya pemberian jaminan kepada pihak ketiga (*relying party*) dari negara dan sebagainya.

Sedangkan untuk tanda tanda tangan elektronik yang berasal dari CA yang tidak berlisensi, saat persidangan harus dibuktikan dahulu bahwa sistem PKI (termasuk standar operasi dan CPS-nya) dari CA yang bersangkutan

[50] *Istilah lain untuk CA berlisesiadalah designated CA (Cayang telah ditunjuk)atau recognized CA(CA yang telah diakui)*

sudah cukup aman (secure). Namun menurut perkiraan kami, pembuktian dengan cara ini amat rentan, karena amat mudah dibantah.

Selain Singapura, Hong Kong juga memiliki skim lisensi yang tidak wajib.

7.3 Cara Penetapan Standar Pengakuan

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

1. Masyarakat yang menetapkan standar pengakuan (customary law)
2. Pemerintah / Negara menetapkan standar dan memberikan lisensi kepada CAs

7.3.1 Penetapan Standar oleh Masyarakat

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

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

7.3.2. Penetapan Standar Baku oleh Negara

Untuk menghasilkan tanda tangan yang ”aman” (secure), maka standar operasi CA tersebut harus diaudit oleh negara. Pada umumnya, auditing ini berkaitan dengan skim lisensi terhadap CA. Jadi dapat disimpulkan di

sini, bahwa negara menjamin keotentikan tanda tangan elektronik yang dihasilkan dari CA yang sudah berlisensi. Italia dan Argentina bahkan hanya mengakui tanda tangan elektronik dari CA yang berlisensi. Disisi ekstrim, Malaysia melarang pendirian CA tanpa lisensi dari pemerintah. Australia tidak memiliki standar baku untuk CA non-pemerintah, namun Australia memiliki standar baku pengopersian CA yang diwajibkan kepada lembaga pemerintah yang operasikan CA. Untuk catatan tambahan, setiap negara bagian di Amerika Serikat tetap diizinkan untuk menetapkan suatu standar tersendiri asal tidak bertentangan dengan undang-undang pemerintahan federal.[51.] Jika sebuah negara bagian memiliki standar sendiri, maka sebenarnya negara bagian tersebut menerapkan 2 standar yang saling melengkapi, yakni standar minimalistik dari pemerintah federal dan standar ketat dari pemerintah negara bagian.

7.4 Skim Pemberian Lisensi & Proses Audit.

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

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

[51.] *One Hundred sixth Congres of the United States of America, Electronic in Signatures in Global and National Commerce*

Mengenai cara melakukan audit ada beberapa cara :

1. Badan yang memberikan lisensi juga melakukan audid
2. Badan pemberi audit menunjuk auditor khusus untuk melakukan audit.

7.5 Analisis Sistem Standar pengakuan yang ada

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

- Sangat efisien secara makro ekonomis, karena tidak perlu birokrasi yang berbelit-belit untuk menjadi CA.
- Selain itu, ada dugaan bahwa kemungkinan sengketa terhadap keotentikan tanda tangan digital juga kecil. Jadi tidaklah perlu melakukan audit yang bertele-tele terhadap CA. Sedangkan keuntungan dari sistem pemberlakuan standar pengakuan tanda tangan elektronik (dengan menggunakan CA berlisensi) yang ketat bagi masyarakat adalah :
- Tingkat keamanan dari tanda tangan elektronik yang terjamin oleh negara
- Kemungkinan manipulasi saat persidangan dapat diminimalisir (karena mengikuti standar baku)
- Mendapatkan asumsi keaslian tanda tangan elektronik dipengadilan (presumption of authencity)

7.6. Penerapan Lisensi Untuk Trusted Third Party

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

Act (Washington: 2000).

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

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

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

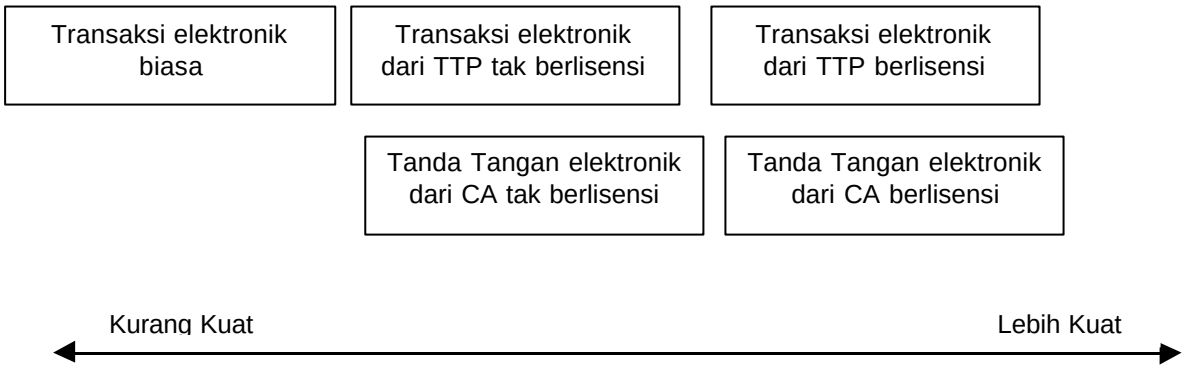
Ada beberapa hal yang kita bisa tarik dari konsep TTP, sehubungan dengan pengakuan keberadaaan hukum transaksi elektonik :

1. Jika benar sebuah kriptografi publik tidak pasti berarti lebih aman ketimbang TTP dengan kunci simetrik, maka seharusnya ada kesempatan bagi TTP dengan kunci simetrik untuk mendapatkan “lisensi” dari negara.

2. Jika ada TTP yang berlinsensi, dan skim lisensi itu tidak wajib, maka ada pula TTP yang tidak berlisensi.

3. Di luar semua itu, ada transaksi elektronik yang tidak melalui TTP apapun (transaksi elektronik biasa). Yang termasuk kategori ini mungkin file di disket dan log transaksi tanpa pengamanan kriptografi atau teknik sekuriti digital lainnya.

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



Gambar 24. Kekuatan pembuktian transaksi elektronik dan tanda tangan elektronik secara hukum

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

Bab 8
Kompatibilitas Hukum Internasional

Secara alami internet memungkinkan kegiatan transnasional yang menghubungkan para pihak yang berasal dari wilayah dan negara yang berbeda yang melewati batas-batas nasionalitas suatu negara. Transaksi dalam Internet dalam pandangan hukum internasional banyak menimbulkan permasalahan yang cukup kompleks, seperti online contract dan online transaction. Jika pihak-pihak yang bertransaksi tinggal dan berada di Indonesia, maka tentu merek tunduk pada hukum Indonesia. Akan tetapi jika para peserta kontrak online (on-line contracting parties) berasal dari negara yang berbeda maka akan lebih susah untuk menentukan kepastian hukum yang akan dipakai (governing law).

Pada bab ini kita akan membalas secara lebih spesifik bagaimana suatu tanda tangan elektronik dapat diakui keberadaannya pada jurisdiksi hukum negara lain.

Jadi, kita bukan mempermasalahkan apa yang harus dilakukan jika terjadi dispute / sengketa terhadap isi kontrak elektonik, namun bagaimana pengadilan dapat mengakui tanda tangan elektronik yang menandakan kesepakatan pada kontrak elektronik tersebut.

Sebelum membahas berbagai macam-macam model pengakuan tanda tangan elektronik, akan kita bahas dasar-dasar model hubungan hukum antar negara, baik dari kacamata hukum publik maupun hukum privat / perdata.

8.1 Hukum Internasional Publik

Prof. Dr. Mochtar Kusumaatmaja S.H., LLM. dalam buku Pengantar Hukum Internasional menyatakan bahwa pengertian hukum internasional publik adalah *"keseluruhan kaedah dan asas hukum yang mengatur hubungan atau persoalan yang melintas batas negara (hubungan internasional) yang bukan bersifat perdata."*

Ruang lingkup hukum internasional publik adalah hukum yang mengatur kegiatan dan kepentingan subyek hukum internasioanl publik, seperti: negara, individu (dalam kepentingan umum seperti perlindungan dari kejahatan), organisasi internasioanal, baik yang berkaitan dengan pemerintah dan non pemerintah (non govermental organization)

8.1.1 Jurisdiksi Internasional

Dalam suatu transaksi elektronik seringkali terjadi tidak ada suatu klausa yang menunjukan pemakaian atau kesepakatan untuk tunduk pada suatu sistem hukum negara tertentu (no express). Jika suatu saat terjadi persengketaan dimana tidak dicantumkan secara nyata governing law-nya, maka harus ada konsepsi hukum untuk penyelesaiannya yang memberikan dasar sistem hukum pengadilan mana yang berwenang untuk memutuskan sengketa yang timbul dari transksi elektronik tersebut dengan wewenang jurisdiksinya.

Suatu pengadilan tidak mempunyai wewenang jurisdiksi terhadap semua orang di dunia. Harus ada sendi yang bersentuhan antara perkara yang diajukan dengan pengasilan yang bersangkutan. Sendi itu adalah :

1. Kewarganegaraan
2. Domisili hukum
3. Perbuatan melanggar hukum
4. Pilihan forum (choice of court)

8.1.2 Perjanjian Internasional

Dalam Artikel 38 Piagam United Convention dinyatakan bahwa perjanjian internasional merupakan salah satu sumber hukum internasional, selain, hukum kebiasaan internasional, doktrin-doktrin para ahli dan yurisprudensi peradilan internasional.

Perjanjian dalam hukum internasional pada awalnya hanya berlaku untuk para pihak yang berstatus negara. Akan tetapi kini organisasi internasional dan warga negara secara internasioanal, telah diakui personalitas hukum internasionalnya. Kesepakatan internasional untuk perjanjian internasional

merujuk pada model law Viena Convention tahun 1949 tentang perjanjian internasional. Indonesia telah meratifikasinya serta membuat UU tentang perjanjian internasional. Di dalamnya mengatur tata laksana pembuatan perjanjian internasional. Secara hukum internasional publik dikenal 2 jenis perjanjian internasional, yaitu:

1. Perjanjian Bilateral dan
2. Perjanjian Multilateral

Kemudian, juga ada yang disebut dengan model law, yang berguna untuk menyelaraskan hukum antar negara dengan ikatan yang relatif longgar.

8.1.2.1 Perjanjian Bilateral

Perjanjian bilateral didefinisikan sebagai perjanjian/kesepakatan yang dibuat oleh dua pihak yang membawa akibat pengikat hanya antar kedua pihak (subyek hukum internasional) atau disebut pacta sun servanda, bahwa perjanjian itu berlaku sebagai undang-undang dan mengikat bagi para pihak yang memperjanjikan.

Hal ini sudah sering dilaksanakan, akan tetapi hanya untuk masalah yang lebih spesifik dan jarang sekali bersifat universal karena hanya berlaku diantara kedua negara tersebut. Sebagai contoh perjanjian pengakuan alat bukti didepan pengadilan masing-masing negara antara Indonesia dengan Kerajaan Thailand, dimana apabila ada penelitian dan penyidikan suatu kejahatan pidana atau perdata antara kedua negara atau antar badan hukum, alat bukti yang ditemukan bisa langsung diterima/diproses di pengadilan negerinya masing-masing tanpa harus lapor dan mendapat pengesahan terlebih dahulu ke kedutaan masing-masing yang penuh birokrasi.

8.1.2.2 Perjanjian Multiteral

Perjanijian multiteral didefinisikan sebagai perjanjian internasional mengenai suatu hal baik dibidang ekonomi maupun politik disuatu bidang (ekonomi,

kelautan, pertahanan dan lain-lain) yang dibuat dan berlaku untuk lebih dari dua negara. Negara peserta dilatar belakangi oleh suatu kesamaan seperti:

1. Regional : ASEAN, APEC
2. Religion : OKI
3. Kepentingan : OPEC, NATO, Pacta Warsawa

Jadi suatu negara dapat menjadi negara kontrak lebih dari satu perjanjian, sesuai dengan kebutuhan negara tersebut.

Suatu negara dapat tunduk dan dapat dikenakan sangsi atas suatu persetujuan / perjanjian internasional dengan beberapa cara :

1. Dengan mengikuti proses pembuatan perjanjian/konvensi dan menjadi negara kontrak, maka legal binding ketika negara tersebut consent to be bound. Meskipun terkait, biasanya tetap ada kesepakatan atau reservation, yakin bisa tidak mengikuti ketentuan suatu pasal dalam perjanjian tersebut, dengan syarat memang diperbolehkan oleh perjanjian tersebut.

2. Tidak mengikuti proses tetapi membuat permohonan untuk dapat ikut serta menjadi negara kontrak dengan meratifikasi perjanjian tersebut dan tetap ada kesepakatan untuk resevasi.

3. Tidak mengajukan keberatan terhadap suatu perjanjian yang menurut konvensi berlaku secara umum, bila negara tersebut tidak melakukan persistent Objection maka aturan / convention tersebut juga berlaku untuknya apabila suatu saat negara ataupun warganya terlibat sengketa yang mengaitkan dengan materi perjanjian tersebut.

8.1.2.3 Model law

Model law dipergunakan sebagai alat untuk menyelaraskan (to harmonize) hukum antar negara. Model law merupakan peraturan yang dibuat oleh forum internasional (subyek hukum internasional) untuk mengatur sesuatu

hal yang menjadi pedoman negara-negara dalam membuat regulasi nasionalnya.

Menurut UNCITRAL[53], model law dituliskan dalam bentuk text perundangan yang kemudian direkomendasikan kepada negara-negara untuk dimasukkan kedalam hukum nasional mereka masing-masing. Tidak seperti konvensi internasional, negara yang menggunakan model law itu untuk memberitahukan kepada negara lain atau PBB bahwa negara yang bersangkutan telah menggunakan model law tersebut. Meskipun demikian, negara-negara disarankan agar tetap memberitahukan sekretariat UNCITRAL tentang penggunaan model law yang dikeluarkan UNCITRAL

Berkaitan dengan masalah transaksi elektronik dan tanda tangan elektronik, beberapa tahap Model Law yang dikeluarkan UNCITRAL:

1. Legal Guide on Electronic Funds Tranfers, (1987)
2. The UNCITRAL Model Law on International Credit Transfer (1992)
3. UNCITRAL Model Law on Electronic Commerce (1996, 1998)
4. UNCITRAL Model Law on Electronic Signature (2000, 2001)

Ketentuan dalam Model Law sifatnya tidak mengikat, akan tetapi apabila telah diadopsi atau merupakan syarat dari perjanjian internasional sebelumnya maka dapat berlaku penuh. Dalam kasus unik ini, para negara kontrak lainnya dapat memaksa negara lain untuk mengikuti standart *model law* tersebut. *Model Law* dapat menjadi hukum kebiasaan internasional bila telah diadopsi oleh banyak negara yang berpengaruh secara ekonomi dan politik dikalangan internasional.

8.2 Hukum Perdata Internasional

Hukum perdata international menurut Prof. Dr. Mochtar Kusumaatmaja S.H LL.M adalah[54]

[53] *http:/www.incitral.org*
[54] *OP.cit, Kusumatmadja*.

" *Keseluruhan kaedah dan asas hukum yang mengatur hubungan perdata yang melintasi batas negara."*

Dalam ruang lingkup hukum perdata internasional adalah hukum yang mengatur kegiatan perdata yang mengandung unsur-unsur internasional atau dengan kata lain melewati batas hukum internasional atau yang melintas dua atau lebih sistem hukum nasional. Perjanjian Internasional juga menjadi dasar kegiatan perdata secara internasional seperti transaksi perdagangan internasional dan kegiatan perdata lainnya.

Subyek hukum perdata internasional melakukan hubungan perdata yang menjadi peristiwa hukum perdata. Hanya saja dalam hukum perdata internasional, peristiwa hukum perdata yang terjadi antara para pihak mengandung unsur-unusr asing atau internasional. Unsur-unsur asing tersebut ditentukan melalui Titik Taut Primer (TTP) dan titik Pertalian Sekunder (TPS). TTP dan TPS tersebut contohnya adalah kewarganegaraan para pihak yang berbeda, pilihan hukum, status personal badan hukum yang berbeda, tempat perbuatan melanggar hukum, tempat kontrak dan pelaksanaan kontrak dibuat, cara penerimaan kontrak, sistem hukum yang berbeda dan sebagainya. Kesemua hal tersebut yang membuat peristiwa hukum tersebut menjadi hukum perdata internasional.

Asas kebebasan berkontrak juga dianut dalam hukum perdata internasional. Maka pilihan hukum dan pilihan forum, merupakan dasar yang penting bagi suatu kontrak atau perjanian para pihak yang secara alamiah mempunyai dan menganut sistem hukum yang berbeda. Pilihan hukum merupakan titik taut penentu dalam menentukan hukum mana yang digunakan dalam suatu perjanjian internasional. Apabila dalam suatu kontrak internasional tidak nampak bahwa para pihak telah memilih hukum tertentu, maka dapat dimengerti orang hendak mencari juga apakah terdapat suatu presumed intention of the parties. Secara tradisional terdapat asas:

a. Lex Loci Contractus, yakni hukum yang digunakan adalah hukum dimana kontrak tersebut dibuat, dan

b. Lex Loci Solutionis, bahwa hukum yang berlaku adalah tempat dimana perjanjian dilaksanakan. Asas ini telah banyak menjadi perdebatan dan sengketa dan menjadi jarang sekali dipakai.

Perkembangan terakhir hukum perdata internasionl memakai asas The Proper Law of the Contract dan The Most Characteristic of the Conection.

8.2.1 The Proper Law of the Contract

Menurut Cheshire[55], yang dimaksud dengan the proper law of the contract adalah :

"…the law or laws by whicb the parties to a contrac itended, or may fairly be presumed to hava itended, the contrac to be governed; or the law or laws to which the paties itended, or may fairly be presumed to have itended to submited them selves."

Berdasarkan pendapat tersebut dapat disimpulkan bahwa pilihan hukum yang akan memayungi perjanjian tersebut harus ditulis dalam perjanjian/ kontrak.

8.2.2 The Most Characteristic of Connection

Yang dimaksud dengan the most characteristic of connection adalah kita melihat kepada faktor-faktor objektif dan keadaan-keadaan sekitar kontrak, melihat konteksnya dan juga bagaimana dapat dilokalisir dalam suatu tempat negara tertentu. Hubungan yang penting diperhatikan adalah antara tempat yang bersangkutan dalam pelaksanaan kewajiban yang karakteristik menurut sifatnya

8.3 Modal Pengakuan Silang Tanda Tangan Elektronik Antara Negara

8.3.1 Pengakuan Melalui Hukum Internasinol Publik

Proses pengakuan atau lisensi, terhadap CA tiap negara diatur masing-masing dengan regulasi lisensi, maupun sistem akreditasi untuk menjadi CA

negara tersebut. Apabila CA pada suatu negara hendak berhubungan dan saling berkomunikasi, maka pengakuan atas CA (berikut keabsahan tanda tangan elektronik yang dihasilkannya) dari luar negeri harus ada, agar CA tersebut dapat dipercaya dan legal.

Hal ini dapat dilakukan dengan adanya adanya suatu perjanjian bilateral antara kedua negara untuk saling mengakui keabsahan dari CA yang ada dimasing-masing negara. Perjanjian ini harus memperhatikan asas hukum kebiasaan internasional, yaitu reciprositas (timbal balik), mutual consent (saling menguntungkan), dan pacta sun servanda (berlaku seperti undang-undang bagi hanya kedua belah pihak).

Modal hubungan yang umum digunakan adalah dengan hubungan pengakuan secara bilateral (dua pihak) dan multilateral. Hubungan ini diklasifikasikan kembali kedalam hubungan bilateral dan multilateral Hukum internasional publik dan hukum perdata internasional.

Agar dapat lebih luas berlakunya dari hanya sekedar hubungan bilateral, seperti regional (ASEAN, European Union dll) ataupun global, maka dapat dibuatkan suatu standar sistem lisensi yang dapat diakui oleh negara-negara peserta konvensi. Hal ini membawa keuntungan bagi subsciber CA untuk dapat berhubungan dengan lebih luas dengan banyak pihak dari subsriber CA berbagai negara. Juga dapat suatu negara memakai rujukan suatu model law (seperti dari UNCITRAL) yang mengatur tentang standar tanda tangan digital dan sertifikatnya, sehingga dapat diakui oleh negara yang mengadopsinya.

8.3.2 Pengakuan Lingkup Hukum Perdata Internasional

Dalam peristiwa pengakuan tanda tangan elektronik yang di buat oleh penyelenggara/ CA yang berbeda status personal hukumnya (mempunyai unsur internasional), maka cara pengakuan yang dapat di lakukan dalam hubungan hukum perdata internasional. Termasuk dalam lingkup ini contohnya adalah penyelenggara CA yang menerbitkan sertifikat untuk web server dan

---

[55] *Cheshire, Internasional Contracts, Glasgow (1948)P. 15, diakutip oleh Sudargo Gautama dalam Hukum Perdata Internasional indonesia cetakan kedua (Bandung, Penerbit Alumni: 1987)*

e-mail (seperti Virisign Trust Network atau Baltimore Omni Root) dan Identrus (CA perbankan internasional).

Dalam melakukan pengakuan tanda tangan elektronik di antara *subscriber* mereka, mereka bisa melakukan hubungan hukum perdata biasa, dengan membuat perjanjian saling mengakui. Yang harus diperhatikan kaedah yang berlaku dalam pembuatan perjanjian tersebut adalah kaedah hukum perdata internasional.

Proses pilihan hukum, pilihan forum dan penyelesaian sengketa alternatif merujuk kepada konvensi perdata internasional yang spesifik. Konvensi jual beli barang Viena Convention 1980, konvensi New York 1958 untuk Arbritrase Internasional dan sebagainya. Namun karena konvensi pilihan hukum untuk pengakuan tanda tangan elektronik sampai saat ini belum ada maka cara pengakuan tanda tangan elektronik harus secara jelas ditulis dalam perjanjian.

Penyepakatan dengan cara apa tanda tangan elektronik diakui perlu dilakukan karena CA maupun *subscriber* tersebut mempunyai status personal yang tunduk pada sistem hukum yang berbeda. Sehingga dalam perjanjian pengakuan harus secara rinci disebutkan aspek-aspek hukum yang akan terjadi apabila terjadi sengketa perdata dikemudian hari seperti: pemakaian hukum negara mana, proses penyelesaian hukum dimana atau model tertentu, maupun apabila selesai dapat atau tidak putusan peradilan asing dapat dilaksanakan di suatu sistem hukum tertentu. Perjanjian yang dibuat oleh para pihak menjadi mengikat para pihak seperti undang-undang dengan asas “Pacta Sun Servanda”

8.3.3 Masalah Sangsi dan Penyelesaian Sengketa

Dalam kegiatan subyek hukum internasional tidak dikenal bentuk penguasa pusat, maka dalam praktek hal pemberian sangsi lebih mengarah kepada pihak yang mempunyai kekuasaan dan kekuatan lebih berat. Akan tetapi ada suatu wanprestasi dari suatu perjanjian maka bila selain alasan force majeur, dapat menyelesaikan sengketanya melalui mekanisme Peradilan Internasional atau Internasional court of Justice, maupun badan arbitrase, mediasi, konsiliasi atau

peradilan internasional seperti Internation Criminal Court, serta Mahkamah Internasional.

8.4 Studi Kasus Pengakuan Silang Tanda Tangan Elektronik

8.4.1 ISETO dan WISeKey

International Secure Elektronic Transaction Organization (ISETO)[56] adalah sebuah yayasan (foundation) / organisasi internasional nirlaba yang berbasis di kota Jenewa, Swiss. ISETO didirikan tahun 1998 dengan tujuan:

- Mempromosikan dan menentukan standar internasional untuk transaksi elektronik yang aman yang berbasis PKI (Global Publik Key Infastructure), termasuk menjadi kustodian untuk Global Common Root untuk CA-CA di dunia ini.
- Membantu menjamin pertumbuhan Internet yang secure di negara berkembang.
- Mengkoordinasikan global information infrastructure.

Global Common Root milik ISETO tesebut dikelola oleh perusahaan swasta bernama WISeKey[57] yang juga berbasis di Swiss. Jadi WISeKey menyediakan layanan root CA bagi CA-CA lain di dunia ini. Harapannya, CA-CA di seluruh dunia dapat saling berhubungan satu sama lain. Kunci privat dari Global Common Root disimpan ditempat yang aman di perut pegunungan Alpen di Swiss.

Salah satu pertimbangan penting mengapa ISETO didirikan di Swiss dan mengelolanya (WISeKey) juga berkedudukan di Swiss adalah karena Swiss adalah negara yang paling netral di seluruh dunia. Bahkan Swiss bukan merupakan anggota dari PBB.
Sedangkan alasan mengapa perlu perusahaan swasta yang mengelola Global Common Root adalah karena asumsi hanya perusahan swasta bisa ‘bergerak cepat’. Jadi jika nanti ternyata WISeKey tidak dapat mengelola

[56] *http://www.iseto.net*
[57] *http://www.wisekey.com*

Global Common Root ISETO, maka pengelola root key tersebut bisa dialihkan ke perusahaan lain.

WISeKey juga telah menandatangan kesepakatan dengan Innnternasional Telecommunication Union (ITU) untuk mempromosikan pengembangan infrastruktur kunci publik (PKI) di 188 negara, dengan maksud memperluas penggunaan transaksi Internet yang aman.

Yang menjadi anggota ISETO adalah negara-negara ataupun orang-orang yang bisa dijamin kenetralannya. Karena itu ada beberapa pendekatan dalam pengakuan tanda tangan elektronik yang menggunakan infrastruktur kunci publik ISETO/ WISeKey.

1. Jika kita memandang bahwa ISETO merupakan organisasi yang anggotanya adalah negara-negara, maka ada harapan untuk menyelaraskan standar tanda tangan elektronik internasional, bahkan sampai pada lapisan template CPS dari WISeKey.
2. Cara kedua adalah melalui ITU (yang sudah jelas beranggotaan negara-negara), membuat semacam model untuk CPS yang standar. Secara praktis, CPS tersebut adalah juga template CPS dari WISeKey.
3. Namun jika ternyata pendekatan melalui hukum internasional publik (butir 1 dan 2 di atas) tidak memungkinkan, mak harus diambil pendekatan pengakuan tanda tangan elektronik melalui hukum perdata internasional.

8.4.2 European Union

Konsep masyarakat Eropa yang bersatu merupakan penyamaan perlakuan di depan hukum masing-masing negara anggota. Directive 1999/93/EC of the Erope Parliament and of the Council on Community Framewrok For Electronic Signatures pada dasarnya bertujuan untuk menyeragamkan tanda tangan elektronik di depan pengadilan negara-negara anggota EU. Hal ini telah ada kesepakatan antara negara Eropa bersatu tersebut yang sifatnya mengikat.

Disini tidak ada organisasi internasional yang berperan, akan tetapi secara multilateral duduk dalam satu meja untuk meyepakati pengakuan tanda

tangan digital dan sertifikat yang dilakukan oleh masing –masing negara-negara anggota forum tersebut.

8.4.3 Verisign Trust Network (VTN dan Baltimore Omni Root)

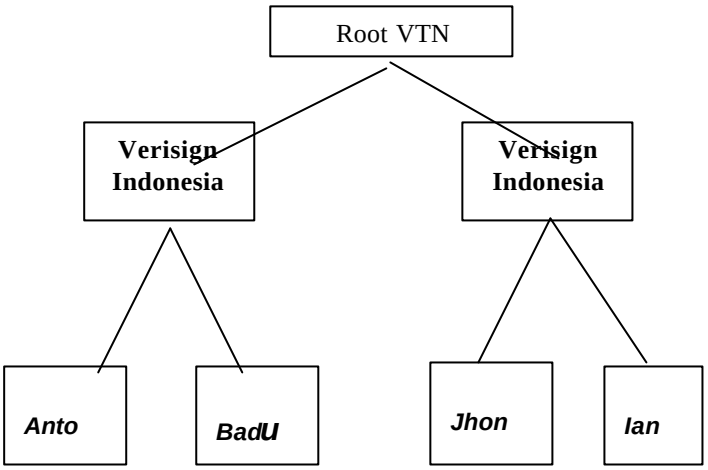
Program Broowser Microsoft Internet Explorer atau Netcape Navigator memanfaatkan protokol SSL (Secure Socket Layer) untuk keamanan transmisi protokol HTTP (Hybertext Transfer Potocol) dari Web server ke browser. Selain itu , aplikasi e-mail client seperti Microsoft Outlook atau Netscape Mail, juga menggunakan trust network keamanan berbasis PKI untuk mengirim secure e-mail berbasis S/MIME.

Untuk melayani penggunaan sekuriti berbasis PKI di Internat, banyak CA yang menyediakan layanan trust network untuk aplikai browser dan e-mail, contohnya Verisign Trust Network[58] (VTN) dan Baltimore Omni Root[59].

Verisign merupakan badan hukum swasta yang berkedudukan (place of bussines) di Amerika dan mengatur hukum Amerika.
Hubungan pengakuan yang mungkin terjadi adalah :

1. Hubungan bilateral privat antara pihak CA swasta Indonesia dengan Root Verisign Truts Network (VTN) di Amerika.
2. Hubungan bilateral private antara CA swasta Indonesia dengan CA swasta negara lain yang merupakan bagian dari VTN
3. Hubungan bilateral privat antara subscrier dari CA swasta Indonesia dengan *subscriber* CA swasta negara lain yang merupakan bagian dari VTN (*subscriber* berbeda domain).

[58] *http://www.verisign.com*
[59] *http://www.baltimore.com*



Gambar 25. Jaring kepercayaan hirarkis dari verisign trut Network

Bila Indonesia terdapat CA yang mengadopsi CPS VTN (misalnya Verisign Indonesia), dan jika hukum Indonesia telah mengakui keberadaan tanda tangan elektronik yang dihasilkan dari PKI Verisign Indonesia, maka menurut pendapat kami pengadilan Indonesia seharusnya mengakui keberadaan tanda tangan elektronik yang dikeluarkan di CA asing yang memakai standar CPS VTN yang sama.

Tetapi hal ini baru dimungkinkan, apabila:

- Standar CPS tersebut benar-benar dipercaya dan diakui oleh pemerintah Indonesia (peraturanya)
- Tidak ada perbedaan yang terlalu mencolok antara CPS Verisign Indonesia dengan CPS asing yang juga tergabung dalam VTN. Atau, jika yang menjadi acuan pemerintah Indonesia adalah CPS dari VTN (bukan CPS dari Verisign Indonesia), maka tidak boleh ada perbedaan mendasar antara CPS asing (ataupun bahkan CPS Verisign Indonesia) dengan CPS VTN. Apabila ada perbedaan yang substansial, maka tetap perlu dibuat perjanjian saling mengakui antara CA yang masih tergabung dalam VTN.

  Selain itu, kita juga bisa melakukan pengakuan tanda tangan elektronik antara dua orang *subscriber* yang berbeda domain (memiliki CA dari 2 CA yang berbeda) dengan cara menjelaskan secara eksplisit dalam perjanjian kerja sama, cara mengakui keabsahan tanda tangan elektronik

jika terjadi sengketa terhadap keabsahan tanda tangan elektronik yang dipergunakan dalam transaksi (hubungan bilateral privat).

8.4.4 Identrus

Identrus LLC (Limited Liability Company)[60] adalah sebuah perusahaan yang mengelola trust network PKI khusus untuk jaringan perbankan. Dimotori oleh bank-bank besar multinasional, yang bisa menjadi CA dalam skenario Indentrus adalah bank-bank peserta identrus. Jaringan kepercayaan Identus menggunakan pola hirarkis, dimana Identruslah yang memiliki root CA-nya, dan bank-bank peserta Idetrus menjadi sub-CA dari Identrus. Hal dapat menjamin kemudahan nasabah dari satu bank untuk berkomunikasi dengan aman dengan nasabah bank lain yang sama-sama bernaung dibawah trust network Identrus. Identrus LLC sendiri berbasis di Amerika Serikat (dengan akta dari negara bagian Dalaware), namun pengelolaan fisik root CA-nya dilakukan oleh perusahaan secure hosting Roccade Megaplex di Apeldoom, Belanda. Identrus sendiri karena melayani sektor perbankan tunduk pada peraturan dari Federal Reserve Bank Amerika Serikat. Mengenai bagaimana cara Indonesia dapat mengakui keberadaan tanda tangan elektronik yang dihasilkan dalam hirarki PKI Identrus,tidaklah jauh berbeda dengan cara pengakuan terhadap model browser based trust network seperti Virisign Trust Network atau Baltimore Omniroot. Artinya jika peradilan di Indonesia sudah mengakui keberadaan Identrus dan mengakui CPS nya, maka secara otomatis peradilan Indonesia akan mengakui keberadaan tanda tangan yang di hasilkan bank-bank yang menjadi sub CA dari Identrus.Selain itu juga dapat pula disepakati dalam perjanjian, cara pengakuan tanda tangan elektronik langsung antar *subscriber* CA.

[60] *http://www.identrus.com*

8.4.5 Model Law on Electronic Signature UNCITRAL (2001)

Dalam dokumen UNCITRAL yang terbaru 2001 tentang model law dari tanda tangan elektronik[61], telah diatur mengenai pengakuan terhadap tanda tangan elektronik asing pada pasal 12. Pada dasarnya model law UNCITRAL tersebut menganjurkan agar tidak ada diskriminasi terhadap tanda tangan elektronik asing dan sertifikat digital asing. Beberapa butir penting adalah :

1. Tempat pembuatan/ penggunaan dari tanda tangan elektronik dan sertifikat digital harus tidak boleh dijadikan pertimbangan hukum sah atau tidaknya tanda tangan atau sertifikat tersebut. Justru yang penting menjadi pertimbangan hukum adalah masalah keamanan teknisnya. (ayat1)

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

3. Untuk menentukan tingkat kehandalan, maka dipergunakan standar–standar rujukan Internasiaonal. (ayat 4) Pasal model law tersebut juga menyebutkan bahwa jika kedua pihak sepakat untuk menggunakan jenis tanda tangan dan sertifikat digital tersebut, maka kesepakatan itu harus dianggap mencukupi untuk melakukan cross border recognition, selama kesepakatan tidak melanggar peraturan lokal. Pada pejelasan pasal 12 tersebut, dijelaskan bahwa, ‘tidak melanggar keharusan peraturan lokal’ sebenarnya merujuk ada peraturan yang tetap mengharuskan pengunaan tanda tangan biasa pada jenis perjanjian tertentu (seperti akta kelahiran, surat nikah, surat tanah dan sebagainya). Disini terjadi semacam ambiguitas dalam pasal 12, karena ayat 2, 3 dan 4 menjelaskan bahwa ada suatu tingkat kehandalan tertentu sebagai syarat pengakuan. Sedangkan pada ayat 5, disebutkan bahwa pengakuan bisa dilakukan langsung antara pihak–pihak yang bertransaksi. Meskipun dijelaskan

bahwa ayat 5 harus memperhatikan ayat-ayat 2, 3 dan 4, namun menurut kami ayat 5 sulit diterapkan, karena memperhatikan prasyarat ayat-ayat sebelumnya. Yang perlu dipahami dari ayat 5 adalah semangat untuk memudahkan cross border recognition terhadap tanda tangan elektronik dan sertifikat digital. Karena jika untuk melakukan pengakuan terhadap tanda tangan elektronik asing harus selalu melalui proses audit dan akreditasi berdasarkan lokal terlebih dahulu, maka hal itu akan menimbulkan ekonomi biaya tinggi, Solusi ideal untuk mencari titik imbang untuk pengakuan tanda tangan asing harus diformulasikan.

[61] *United Nations Commission on International Trade law, Draft Guide to Enactment of the UNCITRAL model law, 38 th*

Bab 9
JAMINAN ASURANSI
DALAM INFRASTRUKTUR
KUNCI PUBLIK

Dalam pelaksanaan transasksi yang menggunakan media elektronik (e-Commerce) dapat saja terjadi hal-hal yang tidak diinginkan oleh para pengguna jasa. Para pengguna jasa perdagangan tersebut adalah para pihak yang mempercayai sistem yang disediakan oleh penyelenggara jasa. Salah satu cara yang dilakukan oleh penyedia jasa untuk memperbanyak pengguna jasa adalah dengan cara memberikan jaminan terhadap keamanan sistem yang diselenggarakan kepada para pengguna jasanya.

Jaminan yang diberikan oleh *Certification Autbority* (CA) dapat berupa *bankers guarantee*, yaitu jaminan penggantian berupa uang kepada *subscriber*. Bentuk penjaminan yang lain nya adalah jaminan yang diberikan oleh perusahaan asurasi kepada CA, *Subcriber* atau *Relying party*.Jaminan atau pertanggungan atas resiko yang akan timbul yang diberikan oleh perusahaan asuransi hanyalah sebatas perjanjian yang dilakukan oleh perusahaan asuransi tersebut dengan yang menjadi tertanggung . Asuransi atau pertanggungan (*Verzekering*) sudah merupakan bagian esensial dan memegang peran penting di dalam perkembangan dan perekonomian, hingga kini perang asuransi sudah di pegang oleh lembaga–lembaga atau institusi-institusi yang mempunyai kemampuan untuk mengambil alih resiko pihak lain[62] Amat penting untuk kita catat bahwa dalam pelaksanaan penjaminan dalam dunia transaksi yang menggunakan media elektronik, asuransi hanya merupakan salah satu pilihan penjamin terhadap segala resiko yang akan timbul.

9.1 Asuransi Secara umum.

Makna penting dari perjanjian asuransi adalah dimana pejanjian tersebut yang memberikan proteksi. Sehingga dapat dikatakan bahwa perjanjian asuransi adalah perjanjian yang menawarkan suatu kepastian dari suatu

---

session (New York:2001),http://www.uncitralorg.

ketidakpastian mengenai kerugian-kerugian bersifat ekonomis yang mungkin timbul karena suatu peristiwa yang belum pasti.

Perjanjian asuransi pada dasarnya merupakan perjanjian penggantian kerugian, dimana penanggung mengikatkan diri untuk mengganti kerugian yang diperkirakan akan terjadi dan akan diderita oleh tertanggung,dimana penggantian kerugian tersebut seimbang jumlahnya dengan kerugian sesungguhnya yang di derita oleh tertanggung .

Perjanjian asuransi termasuk kedalam perjanjian bersyarat dimana kewajiban dari penanggung baru dapat dilaksanakan apabila telah terjadi suatu peristiwa yang mengakibatkan kerugian bagi tertanggung sebagaimana diperjanjikan dalam pertanggungan.

Perjanjian tersebut termasuk dalam perjanjian timbal balik, dimana kewajiban penanggung untuk membayarkan kerugian diikuti oleh kewajiban tertanggung untuk membayar premi kepada penanggung. Syarat-syarat dalam perjanjian asuransi pada dasarnya merupakan kelanjutan dari perjanjian sebagaiman diatur dalam pasal 1320 Kitab Undang-undang Hukum Perdata.

9.1.1 Dasar Hukum asuransi

Di dalam peraturan perundang-undangan Indonesia,asuransi telah memiliki dasar hukum sejak zaman kolonial Belanda, dalam perkembanganya asuransi sudah mempunyai perundang-undanganya sendiri, beserta pengertianya menurut masing-masing perundangan :

1. Berlakunya Kitab Undang- undang Hukum Dagang/ KUHD (*wetboek van Koophandel*) pada tahun 1848, merupakan dasar hukum pertama keberlakuan asuransi di Indonesia.

   Pengertiannya diatur didalam pasal 246:

   > *Asuransi atau pertanggungan adalah suatu perjanjian, dengan mana seorang penanggung mengikatkan diri kepada seorang tertanggung,dengan menerima suatu premi, untuk memberikan penggantian kepadanya karena suatu kerugian, kerusakan,*

[62] *Sri rejeki Hartono,Hikum Asuransi dan Perusahaan Asuransi, (Jakarta: sinar Grafika,1992),hal.*

kehilangan keuntungan yang diharapkan, yang mungkin akan dideritanya karena suatu peristiwa yang tidak tertentu".

2. Kitab Undang-undang Hukum Perdata/ KUHPer (*Burgerlijk Wetboek*/ BW), pengertiannya diatur d dalam pasal 1774 (perjanjian pertanggungan):

   "*Suatu perjanjian untung-untungan adalah suatu perbuatan yang hasilnya, mengenai untung ruginya baik bagi semua pihak, maupun bagi sementara pihak, bergantung dari suatu perjanjian yang belum tentu,*

   Demikian adalah :
   - *Perjanjian pertanggunan*
   - *Bunga cagak hidup;*
   - *Perjudian dan pertaruhan".*

3. UU No 2 Tahun 1992 Tentang Usaha Perasurasian. Pengertian asuransi jauh lebih luas dibandingkan dengan pasal 246 KUHD :

   "*Asuransi atau Pertanggungan adalah perjanjian antara dua pihak atau lebih, dengan mana pihak penanggung mengikatkan diri kepada tertanggung dengan menerima premi asuransi, untuk memberikan penggantian kepada tertanggung karena kerugian, kerusakan atau kehilangan keuntungan yang di harapkan, atau tanggung jawab hukum kepada pihak ketiga yang mungkin akan diderita tertanggung , yang timbul dari sutu peristiwa yang tidak pasti, atau untuk memberikan suatu pembayaran yang didasarkan atas meninggal atau hidupnya seorang yang dipertanggungkan ".*

Dari dasar-dasar pengertian diatas, maka dapat ditarik unsur-unsur dari asuransi, yaitu:

1. Subyek hukum; yaitu penanggung dan tertanggung sebagai para pihak .
2. Premi yaitu sejumlah uang yang harus dibayar oleh tertanggung kepada penanggung.

3. Peristiwa tertentu; yaitu peristiwa yang belum tentu terjadi.
4. Ganti rugi; yaitu pemberian asuransi.

9.1.2 Asuransi sebagai Perjanjian

Berdasarkan dasar-dasar pengertian yang diatur di dalam dasar-dasar hukum asuransi di atas, maka asuransi adalah salah satu bentuk perjanjian. Dengan dasar pengertian demikian, maka perjanjian asuransi, selain mengacu kepada UU No.2 tahun1992 tentang Usaha Perasuransian juga mengacu pada syarat sahnya perjanjian yang diatur oleh pasal 1320-1337 KUHPer.

Para pihak yang membuat perjanjian asuransi juga mempunyai kebebasan mengatur sendiri isi perjanjianya (asas kebebasan berkontrak) dengan berdasar pada pasal 1338 KUHPerdata:

> *"Semua perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya.*
>
> *Suatu perjanjian tidak dapat ditarik kembali selain dengan kedua belah pihak, atau karena alasan- alasan yang oleh undang-undang dinyatakan cukup untuk itu.*
>
> *Suatu perjanjian harus dilaksanakan dengan itikad baik;*

Asuransi dalam terminogi hukum merupakan suatu perjanjian, oleh karena itu perjanjian itu sendiri perlu dikaji sebagai acuan menuju pada pengertian perjanjian asuransi. Disamping itu karena acuan pokok perjanjian asuransi tetap pada pengertian dasar dari perjanjian. Secara umum dapat digambarkan dengan perbuatan dimana satu orang atau lebih mengikatkan dirinya kepada satu orang atau lebih, dimana hubungan hukum yang terjadi antara para pihak tersebut didasarkan pada pihak yang satu berhak untuk mendapatkan suatu prestasi dari yang lain dan pihak yang lain tersebut berkewajiban melaksanakan isi dari perjanjian tersebut.

Dari batsan sebagaimana yang disebutkan sebelumnya, dapat ditarik kesimpulan bahwa setiap perjanjian pada dasarnya akan meliput hal-hal sebagaimana akan dijelaskan berkut ini :

1. Bahwa perjanjian yang dibuat selalu menimbulkan atau menciptakan hubungan hukum.
2. Bahwa perjanjian menunjukan adanya kemampuan atau kewenangan menurut hukum .
3. Bahwa perjanjian mempunyai atau atau berisikan suatu tujuan, bahwa pihak yang satu akan memperoleh prestasi/ pemenuhan kewajiban dari pihak yang lain yang dapat berupa memberikan sesuatu, melakukan sesuatu, atau tidak melakukan sesuatu .
4. Dalam perjanjian, kreditur berhak atas pemenuhan kewajiban dari debitur.
5. Bahwa dalam setiap perjanjian debitur wajib dan bertanggungjawab melakukan kewajibanya sesuai dengan isi perjanjianya.

9.1.3 Objek yang diasuransikan

Yang dijadikan sebagai objek dalam suatu perjanjian asuransi adalah segala sesuatu yang merupakan isi atau bagian dari perjanjian tanggung menanggung antara penanggung dengan tertanggung yang mencakup benda dan jasa, jiwa dan raga, kesehatan manusia, tanggung jawab hukum serta semua kepentingan lainnya yang dapat hilang, rusak, rugi atau berkurang nilainya.

Objek asuransi menurut pasal 268 Kitab Undang–undang Hukum Dagang. Adalah semua kepentingan yang:

a. dapat dinilai dengan sejumlah uang
b. dapat takluk terhadap bermacam-macam bahaya
c. tidak dikecualikan oleh undang-undang.

9.1.4 Subjek Hukum dalam Asuransi

Di dalam asuransi dikenal adanya beberapa subyek (para pihak yang berkepentingan) :

1. Pihak penanggung

Penanggung adalah pihak yang bersedia untuk menerima dan mengambil alih resiko dari pihak lain (tertanggung). Bentuk penerimaan

ini adalah perjanijian antara kedua belah pihak, dimana penanggung bersedia dan berjanji untuk memberikan penggantian (konpensasi) kepada pihak lain (tertanggung) apabila pihak tersebut mengalami kerugian, kerusakan, atau kehilangan keuntungan karena suatu peristiwa yang tidak tertentu, sesuai yang disepakati di dalam perjanjian.

Penanggung dapat berupa pribadi kodrati (perorangan), ataupun berupa badan hukum (perusahaan asuransi).

2. Pihak tertanggung

   Tetanggung adalah pihak yang ditanggung oleh penanggung. Yang dapat menjadi tertanggung adalah pribadi kodrati (perorangan), kelompok orang atau lembaga, Badan Hukum termasuk perusahaan atau siapapun yang dapat menderita kerugian[63]. Berdasarkan pasal 1 butir (7) UU No. 2 tahun 1992 tentang Usaha Perasuransian, maka ditemukan apa yang dikenal sebagai perusahaan reasuransi, yaitu perusahaan yang memberikan jasa dalam pertanggungan ulang terhadap resiko yang dihadapi oleh Perusahaan Asuransi Kerugian dan atau Perusahaan Asuransi Jiwa. Fungsi perusahaan Reasuransi disini adlah pihak (badan hukum bukan perorangan) yang menanggung kerugian yang dialami oleh Perusahaan Asuransi. Jadi dalam hubungannya perusahaan Asuransi adalah pihak tertanggung dan perusahaan reasuransi adalah pihak penanggung.

9.2 Pertanggungan Resiko dalam PKI

Dalam bagian ini dimaksud adalah pertanggungan terhadap segala resiko yang mungkin akan terjadi dalam e-transaction. Pihak–pihak yang dapat menjadi tertanggung dalam pertanggungan dalam transaksi elektronik, khususnya yang tergabung di dalam Publik Key Infrastrukture adalah:

a. Pelanggan (*subcriber*)
b. Otoritas Sertifikasi (Certification Authority)
c. Pihak- pihak ketiga yang berkepentingan (*Relying party*)

[63] *hartono,ibid. Hal 88.*

9.2.1 Hal yang terkait dalam pertanggungan

Subyek Hukum didalam perjanjian asuransi yang berkaitan dengan transaksi elektronik, khususnya yang tergabung di dalam public Key Infrastructure adalah:

1. pelanggan (*subscriber*)

2. Otoritas Sertifikasi (certification authority)
   a. Otoritas Sertifikat sebagai pihak tertanggung
   b. Otoritas Sertifikat sebagai pihak menanggung

3. Pihak-pihak ketiga yang berkepentingan (*relying party*)

9.2.1.1 Pelanggan (*subscriber*)

Pelanggan disini berarti perorangan ataupun badan hukum yang menggunakan jasa daripada otoritas sertifikat dalam melakukan transaksi elektronik untuk alasan keamanan dan sekuritas.
Walaupun terdapat jaminan keamanan dari otoritas sertifikat, pelanggan juga memerlukan jaminan asuransi selain terhadap kemungkinan resiko tidak amannya transaksi elektronik, juga asuransi terhadap kelalaian yang mungkin terjadi dari pihak otoritas sertifikasi.

9.2.1.2 Otoritas Sertifikasi (certification authority)

a. Otoritas sertifikasi sebagai pihak tertanggung

   Otoritas sertifikasi dalam menjalankan usahanya memerlukan jaminan asuransi, terutama terhadap sistem yang dipergunakanya untuk menjamin sekuritas di dalam publik key infrastructure.

b. Otoritas sertifikasisebagai pihak menanggung

   Dalam hal terjadinya bentuk kelalaian yang terbukti karena pihak dari otoritas sertifikasi, maka dalam hal ini pihak pelanggan atau pun pihak lain yang berkepentingan akan menuntut ganti rugi atas

kelalaianya. Dalam hal ini biasanya bentuk asuransi yang di berikan oleh otoritas sertifikasi adalah :

1. Diasuransikan/ ditanggung oleh perusahaan asuransi yang menggung kelalaian dari otoritas sertifikasi .
2. Otoritas sertifikasi tersebut langsung menggung kerugian dalam bentuk reliace limit (akan di bahas lebih lanjut).

9.2.1.3 Pihak- Pihak Ketiga yang Berkepentingan (*relying party*)

Pihak lain yang berkepentingan dalam hal ini adalah para pihak yang secara langsung menghubungkan dirinya dengan *subscriber* dari sebuah CA. Hubungan yang terjadi dapat berupa hubungan transaksi antara pihak yang berkepentingan dengan *subscriber*. Atas segala kemungkinan kerugian yang mungkin terjadi dalam hubungan transaksi yang di lakukan melalui media internet dengan jaringan keamanan yang di sediakan oleh CA, maka pihak yang berkepentingan tersebut dapat mengasuransikan transaksi yang dilakukanya kepada perusahaan asuransi, dengan asumsi bahwa dari transaksi yang di lakukan tersebut, pihak yang berkepentingan tadi dapat menderita kerugian apabia terjadi sesuatu hal yang menyebabkan transaksi tersebut batal karena kelalaian pihak otoritas sertifikat ataukeadaan memaksa lainnya.

9.2.2 Objek yang diasuransikan dalam Transaksi Elektronik

Berdasarkan penjelasan mengenai subyek hukum diatas, maka dapat ditarik objek yang diasuranikan di dalam transaksi elektronik:

1. Transaksi Elektronik

   Transaksi elektronik dapat dijadikan pula objek dari asuransi, dalam arti bahwa resiko yang perlu diasuransikan adalah kerugian yang terjadi dalam hal data (message) yang hendak disampaikan, gagal sampai ke tempat tujuan karena sesuatu hal.

2. Sistem

Suatu otoritas sertifikat menyediakan sarana atau sistem untuk melakukan hubungan telekomunikasi antara para pengguna jasa. Hubungan komunikasi tersebut dapat terjadi kapan saja dan dapat dilakukan oleh siapa saja. Sistem yang disediakan oleh penyedia jasa tersebut dapat mengalami gangguan kerusakan, baik itu bersifat teknis sementara maupun yang bersifat memeksa karena bencana alam misalnya.

9.3 Dasar Hukum Asuransi Dalam PKI

Pada intinya yang peraturan yang mendasari kegiatan perasuransian di Indonesia adalah Kitab undang-undang Hukum Dagang, pada Bab Kesembilan, tentang asuransi atau pertanggungan seumumnya. Penerapannya pada transaksi yang menggunakan media elektronik, dalam ruang lingkup hukum Indonesia, transaksi yang menggunakan media elektronik dapat diasuransikan dengan berdasarkan hukum yang berlaku di Indonesia.

9.3.1 Tentang Polis Asuransi

Menurut pasal 255 KUHD, perjanjian pertanggungan harus diadakan dengan membuat suatu akta, yang disebut polis. Namun tidak dapat ditarik kesimpulan bahwa polis dalam suatu perjanjian pertanggungan itu merupakan suatu syarat untuk adanya perjanjian pertanggungan [64]. Pada KUHD jelas dilihat pada pasal 259 bahwa yang membuat polis adalah pihak tertanggung. Dalam konsep asuransi untuk menanggung kerugian pada transaksi melalui media elektronik maka harus diketahui secara jelas apa-apa saja yang harus dilindungi/ ditanggung oleh perusahaan asuransi.

[64] *Emmy Pangaribuan Simanjuntak, Hukum Pertanggungan (pokok-pokok pertanggungan kerugian, kebakaran dan jiwa), (Yogyakarta: Seksi Hukum dagang Fakultas Hukum Universitas gajah Mada, 1982), hal 20.*

9.3.2 Pertanggungan kaitannya dengan *Relying party*

Perjanjian pertanggungan dapat dilakukan oleh seseorang untuk kepentingan sendiri, akan tetapi juga dapa dilakukan oleh seseorang yang bertindak atas nama orang yang mempunyai kepentingan. Dalam hal ini orang tesebut harus tunduk pada aturan-aturan mengenai pemberian kuasa, sehingga bukanlah ia sendiri yang terkait pada penanggung, akan tetapi adalah orang yang berkepentingan sendiri. Dengan kata lain *Relying party* dapat tersangkut dalam suatu perjanjian pertanggungan antara CA dengan sebuah perusahaan Asuransi, walaupun *Relying party* tersebut sebenarnya dapat melakukan perjanjian pertanggungan sendiri dengan perusahaan Asuransi.

Tetapi bila perjanjian pertanggungan untuk kepentingan pihak ketiga itu dibuat tanpa pemberian kuasa atau diluar pengetahuan orang yang berkepentingan, maka pertanggungan itu batal dengan tidak mengikat waktu dengan mana perjanjian pertanggungan itu diadakan apabila dan sejauh mana kepentingan yang sama oleh orang yang berkepentingan atau oleh orang ketiga atas kuasanya telah dipertanggungkan pada saat sebelum dia menerima pemberitaan tentang pertanggungan yang dibuat diluar pengetahuannya[65].

9.4 Masalah Realiance Limit

Dari sudut pandang CA, menjamin kerugian yang mungkin dialami oleh *relying party* akan sangat mengancam keberlangsungan hidup dari CA itu sendiri, karena mengingat bahwa CPS merupakan perjanjian yang dibuat dari CPS, dimana pihak-pihak yang berhubungan dengan CA tidak disebutkan dengan secara spesifik identitasnya, maka tidak diketahui pula berapa relying parties yang berkepentingan terhadap suatu sertifikat digital seorang *subscriber*, sehingga hal tersebut dapat mengakibatkan kerugian yang sangat besar terhadap CA.

[65] *Ibid, hal.32*

Tetapi di luar negeri, kerugian besar-besaran ini dapat dicegah dengan adanya reliance limit dari pihak CA. Realince limit ini adalah sejenis asuransi namun yang ditetapkan oleh pihak CA itu sendiri (atau ditanggung oleh pihak asuransi), dimana di dalam CPS, jumlah nominal *reliance limit* tersebut telah ditetapkan sebelumnya,dan jika terjadi kerugian akibat dari lalainya pihak CA, maka kerusakan yang dialami oleh relying parties akan diambil dari *reliance limit* tersebut tetapi CA tidak akan bertanggung jawab terhadap kerugian yang diderita diatas dari jumlah nominal reliance limit tersebut. Reliance limit hanya menanggung kerugian 1 (satu) kali transaksi saja. Jadi misalnya, di Utah reliance limit-nya ditetapkan US$ 10.000, maka jika terjadi kerugian karena pihak CA,dan ternyata terdapat 10 pihak relying parties, yang mengalami masing-masing kerugian US$ 5.000, maka CA hanya menanggung maksimum US$ 10.000 dari reliance limit, dan tidak lebih, walaupun kerugian yang dialami oleh pihak relying parties mencapai US$ 5.000.

Untuk mencegah tindakan yang kurang bertanggung jawab dari CA untuk menurunkan nilai nominal dari reliance limit, maka jumlah nominal tersebut biasanya di atur di dalam peraturan pemerintah (PP) negara yang bersangkutan, ataupun ditetapkan di dalam regulasi atau keputusan yang dibuat oleh Badan Pengawas.

KESIMPULAN

Menurut pasal 22 dari *Algemeine van Bapelingen*, seorang hakim tidak bisa menolak kasus bahkan jika belum ada hukum spesifik yang mengatur kasus tersebut. Hakim diwajibkan untuk membuat konstruksi hukum untuk kasus itu berdasarkan hukum yang sudah ada.

Kami telah melakukan identifikasi terhadap konstruksi hukum untuk transaksi elektronik dan tanda tangan elektronik berdasarkan hukum Indonesia. Meskipun ada beberapa cara untuk mengakui keberadaan transaksi elektronik dan tanda tangan elektronik, teknik-teknik tersebut membutuhkan interpretasi hakim yang bisa menjadi sangat subjektif. Masalah lain adalah minimalnya pengakuan eksplisit terhadap keberadaan hukum transaksi elektronik dan tanda tangan elektronik, atau kalaupun ada hanya berlaku pada sektor tertentu saja.

Sangat disayangkan bahwa beberapa kemungkinan yang kami temukan dalam usaha memberikan pengakuan terhadap transaksi elektronik dan tanda tangan elektronik berdasarkan hukum yang ada, bukanlah solusi yang elegan. Hal ini disebabkan karena solusi-solusi tersebut masih masih memberikan kejelasan hukum.

Agar transaksi elektronik dan tanda tangan elektronik dapat diakui dalam pengadilan Indonesia secara tegas, maka kami menyarankan agar perundangan baru harus dibuat untuk menerima transaksi elektronik dan tanda tangan elektronik secara umum.

PENUTUP

Terselesaikannya laporan ini adalah berkat dkungan penuh dari manajemen LKHT-FHUI, yakni Bpk. Freddy Haris, S.H. L.LM selaku ketua LKHT dan Bpk. Edmon Makarim, S.H. S.Kom, selaku ketua harian LKHT. Kami juga berterima kasih kepada Bpk. J. Kriwsanto dan Bpk. Ashar Budiman, directur P.T. Indosatcom Adi Marga, yang telah memberikan bantuan dana yang diperlukan dalam penelitian fase pertama ini.

Secara pribadi, saya (A. M. Wibowo) ingin berterima kasih kepada kedua supervisor saya yakni Dr. Gary Tan dan Associate Professor Dr. Lam Kwok Yan dari School of Computing, National University of Singapore yang telah mengizinkan saya melakukan studi di lapangan di Indonesia pada bulan Juli 2000 sampai November 2000.

Terima kasih pula pada pihak-pihak lain yang telah memberikan koreksi dan bantuan kepada kami, seperti Bpk. Iwan Setiawan dari Bank Indonesia.

Ucapan terima kasih juga kami ucapkan kepada Departemen Perindustrian dan Perdagangan Republik Indonesia yang telah mempercayakan penelitian mengenai kebijakan dan regulasi mengenai tanda tangan digital kepada LKHT-FHUI.

LAMPIRAN : PERBAIKAN VERSI LAPORAN

Versi beta 1.0, 23 April 2001

- pertama kali diserahkan draft ke Deperindag

Versi beta 1.01, 3 Mei 2001

- perbaikan pada keanggotaan WISeKey di bab 8

Versi beta 1.03, 21 mei 2001

- tambahan bab penutup
- tambahan sub-bab"status dokumen" pada bab pendahuluan
- sub-bab3.8.4 judulnya menjadi "Kemungkinan Pengakuakn"
- ditambahkan sub-bab 3.9 berjudul "Pengakuan Transaksi Elektronik Secara Sekteral di Indonesia"
- Sub-bab 4.3.2.2. engenai bea materai elektronik, dipindah kebawah sub-bab 3.9
- Sub-bab 2.4.9, "dienkripsi dengan kunci publiknya" diperbaiki menjadi "private encryption key" menjadi private decryption key"
- Sub-bab 3.2.4, "tidak berdasarkan atas kemauan" menjadi "tidak berdasarkan atas inisiatif"
- Sub-bab 3.3.1, "Pasal-pasal dari hukum perjanjian" dihapus, diganti dengan "Para pihak diperkenankan"
- Sub-bab 3.3.1, disisipkan dalam "melanggar ketertiban umum" menjadi "melanggar aturan yang memaksa (dwigend recht), ketertiban umum"
- Sub-bab 3.3.1. "kita diperbolehkan membuat undang-undang bagi kita sendiri." Menjadi "kita diperbolehkan memperjanjikan sesuatu bagi kita sendiri yang akan berlaku bagi para pihak dan mempunyai kekuatan hukum seperti halnya sebuah undang-undang".
- Sub-bab 3.3.2. ditambahkan setelah "sesuatu formalitas" dengan "tertentu, kecuali untuk beberapa perjanjian yang memang oleh undang-undang dipersyaratkan suatu formalitas tertentu"
- Sub-bab 3.4, dihapuskan kutipan dari pasal 1330, digantu dengan keterangan mengenai kecakapan seseorang menurut KUH Per.
- Sub-bab 3.4, dihapuskan kalimat "sesuatu yang menyebabkan seorang membuat suatu perjanjian"

- Sub-bab 3.5.1, disisipkan dalam “maka perjanjian” menjadi ”maka ada madzhab yang berpendapat bahwa perjanjian”
- Sub-bab 3.5.1, dihapuskan kalimat “patut dicatat, hal ini mengisyaratkan kedua belah pihak”
- Sub-bab 3.7.13, ditembahkan kalimat baru setelah kalimat “Apabilah kita mengartikan syarat ‘ tertulis’ secara harafiah…” yakni ‘tertulis’ disini harus diartikan secara meluas, karena tidak selalu harus menggunakan media kertas. Jadi tertulis disini sebenarnya hanyalah salah satu media fiksasi saja atau perlekatan suatu informasi pada suatu media.”
- Sub-bab 3.7.13, ditambahkan setelah “transaksi elektronik sulit diakui” dengan “sehingga kata ‘tertulis ini’

Versi 1.04,31 Mei 2001.

mengubah format tanggal pencetakan

mengubah kesalahan durasi penelitian menjadi samapai bulan April 2001, pada abstrak dan pendahuluan.

Mengubah judul atas pada halaman sampul dari “Laporan Penelitian Tahap Pertama” “Naskah Akademik Tahap Pertama’. Penelitiannya sendiri tetap berjudul “Kerangka”

Perbaikan pada gambar-gambar yang keterangan gambarnya terpisah dari gambarnya.