Tanda Tangan dan Sertifikat Digital

Dewasa ini, kebutuhan akan kerahasiaan informasi serta penjagaan atas keaslian suatu informasi dirasa semakin meningkat. Pembentukan *framework* untuk otentikasi dari informasi berbasis komputer memerlukan pengetahuan dan ketrampilan akan hukum dan bidang keamanan komputer. Akan tetapi, mengkombinasikan antara kedua hal ini bukan pekerjaan yang mudah. Konsep yang ada di dunia hukum seringkali hanya berkorelasi sedikit dengan konsep yang ada pada dunia keamanan komputer. Sebagai contoh, konsep "tanda tangan digital" (*digital signature*) yang dikenal pada dunia keamanan komputer adalah hasil dari penerapan teknik-teknik komputer pada suatu informasi. Sedangkan di dunia umum, tanda tangan mempunyai arti yang lebih luas, yaitu sebarang tanda yang dibuat dengan maksud untuk melegalisasi dokumen yang ditandatangani.\

Dalam dunia nyata, untuk menjamin keaslian serta legalitas suatu dokumen digunakan tanda tangan. Tanda tangan ini merupakan suatu tanda yang bersifat unik milik seseorang dan digunakan untuk memberi pengesahan bahwa orang tersebut setuju dan mengakui isi dari dokumen yang ditandatangani. Untuk dokumen-dokumen elektronik pun dibutuhkan hal semacam ini. Oleh karena itu, diciptakan suatu sistem otentikasi yang disebut tanda tangan digital. Tanda tangan digital merupakan suatu cara untuk menjamin keaslian suatu dokumen elektronik dan menjaga supaya pengirim dokumen dalam suatu waktu tidak dapat menyangkal bahwa dirinya telah mengirimkan dokumen tersebut. Tanda tangan digital menggunakan algoritma-algoritma serta teknik-teknik komputer khusus dalam penerapannya.

Tujuan Tanda Tangan

Secara umum, penandatanganan suatu dokumen bertujuan untuk memenuhi keempat unsur di bawah ini

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

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

Atribut Tanda Tangan

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

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

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

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

Cara Kerja Teknologi Tanda Tangan Digital

Tanda tangan digital dibuat dengan menggunakan teknik kriptografi, suatu cabang dari matematika terapan yang menangani tentang pengubahan suatu informasi menjadi bentuk lain yang tidak dapat dimengerti dan dikembalikan seperti semula. Tanda tangan digital menggunakan "*public key cryptography*" (kriptografi kunci publik), dimana algoritmanya menggunakan dua buah kunci, yang pertama adalah kunci untuk membentuk tanda tangan digital atau mengubah data ke bentuk lain yang tidak dapat dimengerti, dan kunci kedua digunakan untuk verifikasi tanda tangan digital ataupun mengembalikan pesan ke bentuk semula. Konsep ini juga dikenal sebagai "*assymmetric cryptosystem*" (sistem kriptografi non simetris).

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

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

digunakan untuk membentuk tanda tangan digital. Fungsi hash ini akan menghasilkan "sidik jari" dari suatu dokumen (sehingga unik hanya berlaku untuk dokumen tersebut) yang ukurannya jauh lebih kecil daripada dokumen aslinya serta dapat mendeteksi apabila dokumen tersebut telah diubah dari bentuk aslinya.

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

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

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

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

Proses pembentukan dan verifikasi tanda tangan digital memenuhi unsur-unsur paling penting yang diharapkan dalam suatu tujuan legal, yaitu:

1. **Otentikasi Penandatangan:** Jika pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah yang telah didefinisikan, maka tanda tangan digital akan dapat menghubungkan/mengasosiasikan dokumen dengan penandatangan. Tanda tangan digital tidak dapat dipalsukan, kecuali penandatangan kehilangan kontrol dari kunci privat miliknya.
2. **Otentikasi Dokumen:** Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan tingkat kepastian dan ketepatan yang jauh lebih tinggi daripada tanda tangan di atas kertas.
3. **Penegasan:** Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan. Tindakan ini dapat menegaskan bahwa penandatangan setuju dan bertanggung jawab terhadap isi dokumen.
4. **Efisiensi:** Proses pembentukan dan verifikasi tanda tangan digital menyediakan tingkat kepastian yang tinggi bahwa tanda tangan yang ada merupakan tanda tangan sah dan asli dari pemilik kunci privat. Dengan tanda tangan digital , tidak perlu ada verifikasi dengan melihat secara teliti (membandingkan) antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya seperti yang biasa dilakukan dalam pengecekan tanda tangan secara manual.

Kelemahan dan Keunggulan Tanda Tangan Digital

Kelemahan yang masih menyertai teknologi tanda tangan digital adalah:

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

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

Pelaksanaan teknik tanda tangan elektronik

Hukum positif Indonesia belum pernah memberikan definisi terhadap kata "tanda tangan" yang sesungguhnya mempunyai dua fungsi hukum dasar, yaitu : (1) tanda identitas Penandatangan, dan (2) sebagai tanda persetujuan dari Penandatangan terhadap kewajiban-kewajiban yang melekat pada akta. Berdasarkan kedua fungsi hukum ini maka dapat ditarik suatu definisi sebagai berikut, "tanda tangan adalah sebuah identitas yang berfungsi sebagai tanda persetujuan terhadap kewajiban-kewajiban yang melekat pada akta". Tentunya definisi "tanda tangan elektronik" seharusnya tidak jauh dari definisi di atas; RUU ITE mendefinisikannya sebagai berikut, "Informasi elektronik yang dilekatkan, memiliki hubungan langsung atau terasosiasi pada suatu informasi elektronik lain yang ditujukan oleh pihak yang bersangkutan untuk menunjukkan identitas dan status subyek hukum". RUU ITE memberikan definisi lebih ke sudut teknik, padahal sebuah tanda tangan mempunyai tujuan untuk menerima/menyetujui secara meyakinkan isi dari sebuah tulisan. Hal ini sangat logis, di mana tanda tangan elektronik mempunyai dua fungsi hukum dasar[6]. Oleh karenanya, Penulis mencoba untuk memberikan definisi sebagai berikut, "tanda tangan elektronik adalah sebuah identitas elektronik yang berfungsi sebagai tanda persetujuan terhadap kewajiban-kewajiban yang melekat pada sebuah akta elektronik. Dia terbuat dari prosedur identifikasi handal dan mampu menjamin hubungan antara akta elektronik dan tanda tangan elektronik. Prosedur ini dianggap handal, kecuali terbukti sebaliknya, selama memenuhi ketentuan-ketentuan yang diatur oleh undang-undang ini".

Untuk mendapatkan kekuatan hukum dan akibat hukum yang sama dengan tanda tangan manuskrip, sebuah tanda tangan elektronik harus mampu memberikan jaminan integritas dari akta elektronik dan mampu mengidentifikasi si Penandatangan dari akta elektronik ini

Jaminan integritas dari akta elektronik

Pasal 11 RUU ITE menentukan bahwa, "Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi ketentuan dalam undang-undang ini", ketentuan-ketentuan yang dimaksud dimuat dalam Pasal 13 RUU ITE yang salah satunya adalah tanda tangan elektronik tersebut harus menjamin integritas dari suatu akta elektronik yang dilekatinya. Jaminan ini dapat dicapai hanya dengan menggunakan teknik kriptologi. Kriptologi (*cryptologie*)

berasal dari bahasa yunani, yaitu *"kryptos"*(disembunyikan) dan *"logos"* (ilmu) yang artinya adalah ilmu dari penulisan-penulisan rahasia, dan dokumen-dokumen terenkripsi dengan kata lain kriptologi merupakan kombinasi dari kriptografi(*cryptographie*) dan kriptanalis(*cryptanalyse*).

Teknik kriptologi bukanlah sebuah teknik baru, ia telah digunakan sejak jaman Julius Cesar, tetapi pada jaman ini, teknik kriptologi yang digunakan masih konvensional. Pengkodean pesan rahasia yang digunakan adalah algoritma yang berasal dari penggesaran abjad-abjad. Kunci rahasia untuk mendekripsi pesan rahasia ini adalah jumlah karakter yang digeser. Contohnya, kata "LQGRQHVLD" merupakan kata rahasia dari INDONESIA, sehingga hanya orang-orang yang mengetahui kunci "penggeseran 3 huruf" yang dapat mengerti tulisan tersebut.

Tentunya di jaman teknologi informasi ini, teknik kriptologi modern yang digunakan. Berkaitan dengan keamanan pesan rahasia, teknik kriptologi modern menjamin sedikitnya lima keamanan minimal, yaitu :

1. Keotentikan (*l'authenticité*), penerima pesan harus mengetahui siapa pengirim pesan tersebut dan harus benar-benar yakin bahwa pesan tersebut berasal dari pengirim;
2. Integritas (*l'intégrité*), penerima harus yakin bahwa pesan tersebut tidak pernah dirubah, atau dipalsukan oleh pihak beritikad tidak baik;
3. Kerahasiaan (*la confidentialité*), pesan tersebut harus tidak dapat dibaca oleh pihak yang tidak berkepentingan;
4. Tidak dapat disangkal (*la non repudiation*), pengirim tidak dapat menyangkal bahwa bukan dia yang mengirim pesan tersebut ;
5. Kontrol akses (*le contrôle d'accès*), sistem kriptologi mempunyai kemampuan untuk memberikan otorisasi ataupun melarang atas setiap akses ke pesan-pesan tersebut.

Bentuk kriptologi

Ada dua bentuk kriptologi yang paling dikenal, yaitu kriptologi simetris dan kriptologi asimetris tetap hanya bentuk terakhir yang digunakan pada tanda tangan elektronik.

Dua bentuk yang paling dikenal dalam teknik kriptologi

Kriptografi simetris hanya menggunakan sebuah kunci rahasia untuk mengenkripsi dan mendekripsi sebuah pesan. Salah satu algoritma simetris yang digunakan

adalah *Data Encryption Standard* (selanjutnya disebut DES) yang mempunyai panjang kunci 64 bit. Teknik ini sudah semakin ditinggalkan karena tingkat kebocorannya sangat tinggi. Bila kunci rahasia tersebut diketahui oleh pihak ketiga maka dia dapat menggunakannya untuk mendekripsi, membaca bahkan memalsukan pesan rahasia tersebut. Untuk keluar dari kesulitan ini digunakanlah sebuah teknik pengkodean yang disebut kriptologi asimetris.

Tahun 1976, dua ahli matematika Diffie dan Hellman memperkenalkan sebuah sistem kriptologi asimetris atau kriptologi kunci publik, teknik ini menggunakan dua buah kunci. Konsep ini kemudian diaplikasikan oleh Rivest, Shamir dan Adleman, dengan membuat sebuah algoritma asimetris RSA pada tahun 1977. Sebuah kunci RSA mempunyai panjang kunci yang bervariasi mulai dari 40 bits hingga 2048 bits[12]. Berkat algoritma ini, Phil Zimmerman mampu membuat sebuah piranti lunak yang diberi nama *Pretty Good Privacy* (selanjutnya disebut PGP). Karena piranti lunak ini didistribusikan secara bebas dan gratis[13] maka penyebaran piranti lunak ini sangat cepat di kalangan pengguna pribadi.

Gambar : kriptologi asimetris

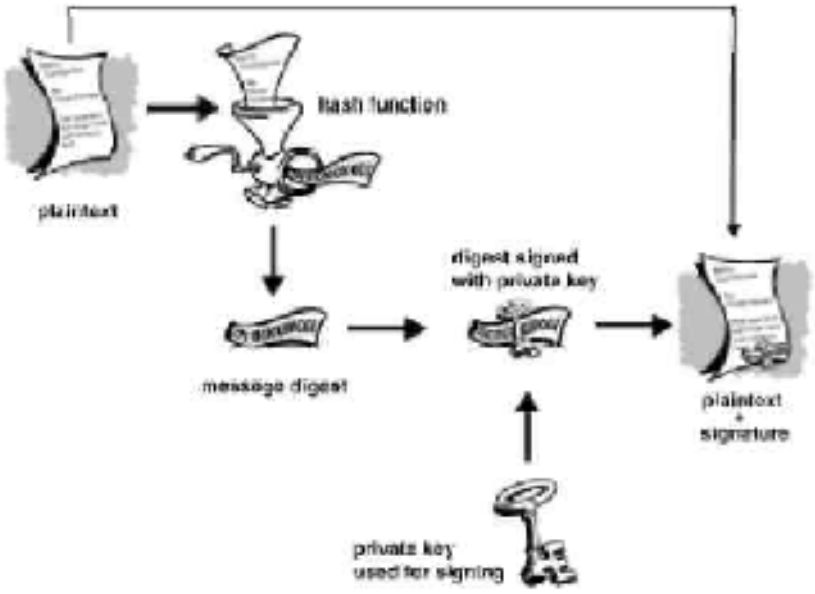
Proses ini melibatkan dua buah kunci, yang disebut kunci privat dan kunci publik. Kunci privat digunakan untuk mengenkripsi pesan rahasia sedangkan kunci publik digunakan untuk mendekripsi pesan rahasia tersebut agar dapat dibaca. Begitupun sebaliknya, kunci publik digunakan untuk mengenkripsi sebuah pesan rahasia dan kunci privat digunakan untuk mendekripsikan pesan tersebut.

Sekalipun secara matematis, dua kunci ini saling berhubungan tetapi tidak dimungkinkan menemukan kunci privat dengan menggunakan kunci publik, sehingga sangat

dimungkinkan untuk mendistribusikan seluas-luasnya kunci publik. Namun sebaliknya, kunci privat harus disimpan dan dijaga kerahasiaannya. Teknik kriptologi asimetris ini merupakan dasar dari pembuatan tanda tangan elektronik.

Proses tanda tangan elektronik

Untuk menandatangani secara elektronis sebuah pesan, dengan bantuan piranti lunak, pengirim akan membuat pertama-tama sebuah *message digest*[16] dari pesan yang asli dengan menggunakan *fonction de hachage* (*hash* dalam bahasa inggris). *Message digest* dari setiap pesan asli adalah unik layaknya "sidik jari", sehingga perubahan sekecil-kecilnya pada sebuah *message digest* akan mengakibatkan perubahan "sidik jarinya" pula. Keuntungannya, baik sang Pengirim maupun Penerima dapat mengetahui keintegritasan pesan tersebut.



Gambar: Tanda tangan elektronik

Selanjutnya *message digest* tersebut akan ditanda tangani dengan menggunakan kunci privat pengirim, dengan kata lain tanda tangan elektronik adalah *message digest* yang dienkripsi oleh kunci privat Pengirim. Kemudian pesan asli dan tanda tangan elektronik dikirim bersama-sama ketujuan yang diinginkan. Berkat kunci publik dari Pengirim yang dikomunikasikan terlebih dahulu ke penerima pesan, Penerima dapat mendekripsi tanda tangan elektronik tersebut, katakanlah hasilnya

D1, selanjutnya penerima akan membuat *message digest* pada pesan asli yang diterima, katakanlah hasilnya D2. Maka langkah terakhir adalah membandingkan keduanya, yaitu D1 dan D2. Bila keduanya memiliki "sidik jari" yang sama, maka dapat dipastikan bahwa itu pesan asli dan belum pernah dirubah (lihat lampiran I dan II tentang penggunaan tanda tangan elektronik). Sekalipun begitu, proses ini tidak dapat mengotentifikasi identitas penulis pesan tersebut.

Pengidentifikasian penulis akta elektronik

Pasal 13 ayat (1) butir (a) dan (b) RUU ITE menentukan sebagai berikut :

(a) Data pembuatan tanda tangan terkait hanya kepada Penandatangan saja;
(b) Data pembuatan tanda tangan elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penandatangan;
(c) […]

(e) Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatangannya;
(f) Terdapat cara tertentu untuk menunjukkan bahwa Penandatangan telah memberikan persetujuan terhadap informasi elektronik yang terkait.

Ketentuan-ketentuan Pasal 13 merupakan syarat-syarat minimal[19] yang harus dipenuhi sebuah tanda tangan elektronik sebelum menikmati "asas praduga kehandalan" (*présomption de fiabilité*) yang memberikan kekuatan hukum dan akibat hukum yang sama dengan tanda tangan manuskrip. Menurut Penulis, penggunaan kata "data pembuatan tanda tangan elektronik" hendaklah disederhanakan menjadi "tanda tangan elektronik", agar lebih jelas dan mudah dimengerti karena tidak ada tanda tangan elektronik tanpa data.

Selain itu, menurut Penulis, butir (f) sebaiknya dihapus karena dari sudut pandang teknis, butir (e) sudah cukup untuk membuktikan bahwa Penandatangan telah memberikan persetujuannya dengan menandatangani akta elektronik tersebut dengan tanda tangan elektronik miliknya. Namun, untuk membuktikan apakah persetujuan Penandatangan tersebut datang tanpa unsur paksaan, digunakanlah fakta-fakta hukum dalam proses peradilanlah, bukan piranti lunak yang digunakan.

Kesempurnaan prosedur identifikasi Penandatangan sangat penting dalam penggunaan tanda tangan elektronik. Jika Hakim meragukan kehandalan prosedur

ini, maka ia akan menolak secara tegas validitas dari akta elektronik yang ditandatangani secara elektronis. Pengidentifikasian Penandatangan dari sebuah akta elektronik dan hubungan antara kunci publik dan subyek hukum membutuhkan bantuan dari pihak ketiga yaitu, Penyelenggara Sertifikasi Tanda Tangan Elektronik (1.2.2.) dengan bantuan sebuah sertifikat elektronik (1.2.1.).

Sertifikat elektronik

Sertifikat elektronik menduduki peran layaknya "paspor elektronik", ia tidak dapat dipisahkan dari praktek tanda tangan elektronik, ia membawa kekuatan hukum yang kuat karena dapat meyakinkan identitas Penandatangan. Sertifikat elektronik mempunyai sebuah struktur internal, artinya ada beberapa bagian yang diwajibkan untuk diinformasikan atau dilekatkan pada sertifikat tersebut untuk memberikan kekuatan hukum pada sertifikat tersebut Syarat-syarat ini akan diatur lebih lanjut di Peraturan Pemerintah berdasarkan Pasal 13 ayat (2) RUU ITE.

Struktur internal ini didefinisikan oleh sebuah norma internasional yang disebut *recommendation X-509 V.3 de l'Union internationale des télécommunications.* Norma internasional ini kemudian dikembangkan oleh *Internet Engineering Task Force* untuk diaplikasikan pada teknologi tanda tangan elektronik. Sebuah sertifikat elektronik, menurut norma X-509 V.3 hendaknya memuat minimal keterangan-keterangan sebagai berikut :

(a) Versi sertifikat;
(b) Nomor seri sertifikat;
(c) Algoritma yang dipergunakan;
(d) Nama pemilik sertifikat digital, temasuk didalamnya keterangan tentang negara asal, organisasi dan seterusnya;
(e) Nama lembaga yang menerbitkan sertifikat elektronik:
(f) Ektensi, disesuaikan dengan kebutuhan.

RUU ITE tidak mempresisikan keterangan-keterangan apa saja yang harus dimuat dalam sebuah sertifikat elektronik, tetapi RUU menyerahkan kepada Peraturan Pemerintah untuk menentukan lebih lanjut mengenai penyelenggaraan sertifikasi elektronik[21].

Namun ada baiknya kita "melirik" Dekrit Komisi Negara Perancis 2001-272 tanggal 30 Maret 2001 tentang "aplikasi Pasal 1316-4 *Code civil* dan tentang tanda tangan elektronik". Pasal 6 dekrit ini menentukan keterangan-keterangan yang

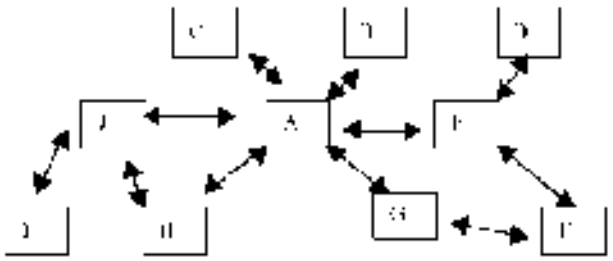
harus dimuat dalam sebuah sertifikat elektronik terkualifikasi adalah sebagai berikut :

(a) Keterangan yang mengindikasikan bahwa sertifikat ini dikeluarkan sebagai sertifikat elektronik terkualifikasi;
(b) Identitias dari Penyelenggara Sertifikasi Tanda Tangan Elektronik serta Negara di mana ia berada;
(c) Nama Penandatangan atau nama aliasnya, disertai dengan bukti-bukti identitas Penandatangan ;
(d) Bila keadaan memungkinkan, keterangan kualitas si Penandatangan sesuai dengan penggunaan daripada tujuan pemakaian sertifikat elektronik itu ditujukan;
(e) Data-data pemeriksa kebenaran/keabsahan tanda tangan elektronik yang sesuai dengan data-data pembuatan tanda tangan elektronik;
(f) Indikasi awal berlaku dan berakhirnya validitas dari sertifikat elektronik;
(g) Kode identitas dari sertifikat elektronik;
(h) Tanda tangan elektronik “sécurisée“ dari Penyelenggara Sertifikasi Tanda Tangan Elektronik yang mengeluarkan sertifikat elektronik tersebut ;
(i) Bila keadaan memungkinkan, disertakan kondisi-kondisi penggunaan sertifikat elektronik, khususnya besarnya transaksi maksimal yang dapat dilakukan denganmenggunakan sertifikat elektronik tersebut.

Web of trust

Sistem sertifikasi tanda tangan elektronik dengan cara-cara di atas memakan biaya yang tidak murah dan tampaknya “hanya” ditujukan kepada kaum profesional saja, sehingga para pengamat berusaha untuk mengurangi biaya tersebut dan memasyarakatan penggunaan sertifikat elektronik dengan mengembangkan sebuah model sertifikasi yang dikenal dengan nama *web of trus*.

Model sertifikasi *web of trust* yang dikembangkan oleh PGP tidak lain adalah model kepercayaan komulatif. Dalam sistem ini, setiap orang dapat bertindak sebagai “pemberi sertifikat elektronik”, dan setiap orang dapat mensertifikasi kunci publik dari pengguna lainnya. Cara kerjanya sebagai berikut, I dapat bertransaksi dengan A karena ada jalur kepercayaan melalui J. Sedangkan antara I dan J telah saling mempercayai kunci publik satu dengan yang lainnya, bila J menandatangani kunci publik I maka A dapat mempercayai I.



Gambar: web of trust

Peraturan Pemerintah tentang penyelenggaraan sertifikasi elektronik kelak sebaiknya mengatur secara spesifik mengenai sistem sertifikasi yang digunakan. Penulis bertanya-tanya, bagaimana validitas juridis dari sebuah prosedur identifikasi dengan menggunakan sistem ini? Bagaimanakah pengguna dapat yakin bahwa setiap orang di jaringan ini *capable* untuk menjalankan perannya sebagai "pemberi sertifikat elektronik" ? Bagaimana pengguna bisa yakin atas kebenaran identitas Penandatangan jika *certification path*[27] telah berada terlalu jauh dari pengguna, misalnya I dan D (lihat gambar).

Sistem ini memang cukup "berani" tapi masih bersifat "utopi", dia tidak dapat memberikan jaminan apapun untuk meyakinkan identitas seseorang. Sistem ini juga hanya berjalan di jaringan Internet, sehingga proses sertifikasi ini tidak di bawah kontrol nyata dan serius. Salah satu karakter dari Internet adalah hilangnya perbatasan (*frontier)* suatu negara, sehingga individu-individu yang berperan sebagai "penyelenggara sertifikasi elektronik" dapat berada di negara manapun. Sebaliknya, hukum mengenal *frontier* sehingga bila terjadi sengketa hukum, pihak-pihak yang dirugikan akan menemui kesulitan untuk meminta tanggung jawab individu-individu "penyelenggara sertifikasi elektronik" yang tinggal di luar negeri. Karena hal ini lah, sistem *web of trust* belum diaplikasikan secara menyeluruh di dunia.

Penyelenggara Sertifikasi Tanda Tangan Elektronik

Penyelenggara sertifikasi elektronis, menurut RUU ITE, adalah subyek hukum yang berfungsi sebagai pihak ketiga yang layak dipercaya, yang menyelenggarakan tanda tangan elektronik untuk Penandatangan dan memastikan identitas dan status subyek hukum Penandatangan tersebut selama keberlakuan tanda tangan elektronik[34]. Definisi ini mengaburkan tujuan utama yang diperankan oleh "penyelenggara sertifikasi elektronis" yaitu menerbitkan sertifikat elektronik

atas tanda tangan elektronik, karena identitas dan status subyek hukum Penandatangan dipastikan ketika diterbitkannya sertifikat elektronik.

Selain tujuan utama ini, penyelenggara sertifikasi elektronis dapat menyediakan pelayanan-pelayanan lainnya yang bertujuan untuk menunjang penyelenggaraan tanda tangan elektronik agar mampu mengikuti evolusi teknologi, misalnya dengan menyediakan jasa "*horodatage*[35]" (dalam bahasa inggris, *time stamping*), jasa pembuatan kunci publik, pengarsipan elektronis[36] dan lain-lainnya. Sehingga, menurut Penulis, lebih tepat Pasal 1 butir(8) ini didefinisikan sebagai berikut, "subyek hukum yang berfungsi sebagai pihak ketiga yang layak dipercaya, yang menerbitkan sertifikat elektronik dan yang menyediakan pelayanan-pelayanan yang berkaitan dengan penyelenggaraan tanda tangan elektronik ». Setelah melihat aspek-aspek teknik dari tanda tangan elektronik, pembahasan ini akan masuk pada aspek-aspek juridis dari tanda tangan elektronik.

Landasan juridis tanda tangan elektronik

Teknologi-teknologi dan media-media baru semakin luas dipergunakan dalam praktik perdagangan, baik di tingkat nasional maupun di tingkat internasional[37], sehingga Organisasi-organisasi internasional semakin memikirkan pengakuan hukum terhadap akta terdematerialisasi dan tanda tangan elektronik. Akhirnya, dorongan datang dari Komisi Perserikatan Bangsa-Bangsa untuk hukum dagang internasional (selanjutnya disebut UNCITRAL) yang mengeluarkan *UNCITRAL Model Law on Electronic Commerce* pada tanggal 16 Desember 1996.

Model law ini sesungguhnya ditujukan untuk menawarkan model hukum kepada negara-negara yang sudah ataupun belum mempunyai peraturan perundang-undangan terhadap materi ini. Namun *model law* sifatnya bebas, artinya negara-negara dibiarkan bebas mau mengikutinya atau tidak. Berkat *model law* ini, banyak negara di dunia berbenah-benah diri, mereka memandang bahwa hukum pembuktian tradisional tidak mampu lagi beradaptasi dengan model perdagangan elektronik, pemerintahan elektronik serta pertukaran yang terdematerialisasi[38]. Oleh karena itu, sangat dibutuhkannya produk hukum yang bertujuan untuk meningkatkan keamanan dari transaksi-transaksi elektronik melalui jaringan elektronik, serta untuk memberikan pengakuan terhadap kekuatan hukum dari alat bukti elektronik dan tanda tangan elektronik, misalnya Komunitas Eropa dengan *Directive communautaire 1999/93/CE du 13 décembre 1999* tentang "tanda tangan

elektronik", Perancis dengan *Loi du 13 mars 2001* tentang "pengadaptasian hukum pembuktian dalam *Code civil français* terhadap teknologi informasi dan tentang tanda tangan elektronik", Malaysia dengan *Digital signature act 1997*, Singapura dengan *Electronic transaction act 1998* dan *Electronic signatures in global and National Commerce Act 30 juin 2000*.

Bagaimana dengan Indonesia ? Hukum acara positif Indonesia baik hukum acara perdata maupun hukum acara pidana belum mengakui alat bukti elektronik dan tanda tangan elektronik padahal dalam transaksi perdagangan elektronik, bahkan pemerintahan elektronik, secara keseluruhan dilakukan tanpa kertas (*paperless*). Berdasarkan Pasal 164 *Herzien Inlands Reglements* (selanjutnya disingkat HIR) dan 1903 Kitab Undang-undang Hukum Perdata (selanjutnya disingkat KUHPerdata) ada 5 alat bukti, yaitu :

(a) Bukti tulisan;
(b) Bukti dengan saksi;
(c) Persangkaan-persangkaan;
(d) Pengakuan;
(e) Sumpah

Bertolak dari ketentuan di atas, jelaslah pengajuan tanda tangan elektronik yang melekat pada akta elektronik di muka pengadilan sebagai alat bukti akan menemukan hambatan dan mengalami proses pembuktian yang rumit, bahkan Hakim dan pihak lawan kemungkinan besar akan menolaknya. Akibatnya, timbul ketidakpastian hukum terhadap akta elektronik dan tanda tangan elektronik, yang ironisnya, berbanding terbalik dengan semakin meluasnya penggunaan akta elektronik dan tanda tangan elektronik dalam transaksi elektronik baik dalam negeri maupun dengan luar negeri.

Revisi hukum pembuktian tentu saja membutuhkan waktu yang tidak singkat, karena itu sambil menunggu disahkannya RUU ITE, maka peranan suatu yurisprudensi tetap sangat dibutuhkan dalam mengisi *recht-vacuum*[39], seperti yang dikemukakan oleh Van Apeldoorn, "Bilamana sesuatu peraturan yang tercantum dalam keputusan Hakim tetapi diturut, jadi, pada kenyataannya peraturan itu telah menjadi bagian dari keyakinan-hukum umum, yakni apabila tentang soal yang bersangkutan telah ditimbulkan suatu yurisprudensi tetap, maka peraturan itu telah menjadi hukum.

Yurisprudensi tetap dapat tercipta, asalkan ahli hukum dan ahli teknologi informasi mampu memberikan sesuatu pemahaman yang mendalam kepada masyarakat pada umumnya, dan kepada para Hakim pada khususnya. Pemahaman yang membawa keyakinan bahwa akta elektronik dan tanda tangan elektronik dapat diterima sebagai alat bukti elektronik, dalam artian ia mempunyai kekuatan hukum yang sama dengan alat bukti tradisonal, selama alat bukti elektronik ini menggunakan proses yang handal yang mampu memberikan jaminan secara meyakinkan identitas pembuat/penulisnya dan integritas dari akta elektronik tersebut.

Tanda tangan elektronik sebagai alat bukti dan kekuasaan Hakim

Berdasarkan Pasal 4 ayat (1) RUU ITE, informasi elektronik memiliki kekuatan hukum sebagai alat bukti yang sah, bila informasi elektronik ini dibuat dengan menggunakan sistem elektronik yang dapat dipertanggungjawabkan sesuai dengan perkembangan teknologi informasi[42]. Bahkan secara tegas, Pasal 6 RUU ITE menentukan bahwa "Terhadap semua ketentuan hukum yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli selain yang diatur dalam Pasal 4 ayat (4), persyaratan tersebut telah terpenuhi berdasarkan undang-undang ini jika informasi elektronik tersebut dapat terjamin keutuhannya dan dapat dipertanggungjawabkan, dapat diakses, dapat ditampilkan sehingga menerangkan suatu keadaan".

Jika RUU ITE telah menjadi hukum positif, saat itu juga akta elektronik dianggap sama dengan akta konvensional, begitu pula dengan tanda tangan elektronik akan dianggap sama dengan tanda tangan manuskrip. Namun dengan hukum acara perdata yang ada saat ini, apakah akta elektronik dapat dianggap sama dengan alat bukti tertulis klasik ? Apakah kekuatan hukum dari akta elektronik tersebut sama dengan kekuatan hukum alat bukti tertulis dalam acara perdata ?

Sesungguhnya pandangan yang mengatakan tanda tangan elektronik tidak dapat menjadi alat bukti tertulis tidaklah mutlak, karena sangat tidak relevan di jaman teknologi tetap memandang alat bukti tertulis dengan cara pandang tahun 1848 ! Disinilah Hakim dituntut untuk berani melakukan terobosan hukum, karena dia yang paling berkuasa dalam memutuskan suatu perkara dan karena dia juga yang dapat memberi suatu *vonnis van de rechter*[44] yang tidak langsung dapat didasarkan atas suatu peraturan hukum tertulis atau tidak tertulis. Dalam hal ini, Hakim harus membuat suatu peraturan sendiri (*eigen regeling*)[45]. Tindakan seperti ini, menurut

Pasal 14 Undang-Undang Nomor 14 Tahun 1970 tentang kekuasaan kehakiman, dibenarkan karena seorang Hakim tidak boleh menolak untuk memeriksa, mengadili dan memutuskan suatu perkara dengan alasan peraturan perundang-undangan yang tidak menyebutkan, tidak jelas, atau tidak lengkap (asas *ius curia novit*). Bil keputusan Hakim yang memuat *eigen regeling* ini dianggap tepat dan dipakai berulang-ulang oleh Hakim-hakim lainnya, maka keputusan ini akan menjadi sebuah sumber hukum bagi peradilan (*rechtspraak*).

Dengan dasar-dasar di atas, seorang Hakim diberikan keleluasan untuk menemukan hukum (*rechtsvinding*), baik dengan cara melakukan interpretasi hukum (*wetinterpretatie*) , maupun dengan menggali, mengikuti dan memahami nilai-nilai hukum yang hidup dalam masyarakat. Metoda interpretasi yang dapat digunakan dalam pencarian kekuatan hukum dari akta elektronik dan tanda tangan elektronik khususnya adalah interpretasi analogi, interpretasi ekstensif dan interpretasi sosiologis[47]. Metoda interpretasi analogis dilakukan dengan memberi ibarat terhadap suatu kata-kata sesuai dengan asas hukumnya, sehingga suatu peristiwa yang pada awalnya tidak dapat dimasukkan, lalu dianggap sesuai dengan ketentuan peraturan tersebut, misalnya menyambung aliran listrik dianggap mencuri/mengambil aliran lisrik sebagaimana yang ditegaskan dalam yurisprudensi tetap *Hoge Raad der Nederlanden* (pengadilan tertinggi di Belanda). Berdasarkan asas konkordansi, pengadilan Indonesia menggunakan yurisprudensi ini untuk menjawab kebingungan Hakim dalam menyelesaikan kasus penyalahgunaan/pencurian listrik.

Berkaitan dengan tanda tangan elektronik, seorang Hakim dapat menggunakan metode interpretasi analogis dengan memperhatikan pandangan dari Pitlo dan definisi yang diberikan oleh *Code civil* Perancis. KUHPerdata dan HIR tidak memberikan definisi yang jelas apa yang dimaksud dengan “tulisan”. Pitlo dalam bukunya *Bewijs en Verjaring naar het Nederlands Burgerlijk Wetboek* mendefinisikannya sebagai berikut “surat sebagai, pembawa tanda tangan bacaan yang berarti, yang menterjemahkan suatu isi pikiran. Atas bahan apa yang dicantumkannya tanda bacaan ini, adalah tidak penting”, serupa dengan Pitlo, Pasal 1316 *Code civil* Perancis menentukan, “*la preuve littérale, ou preuve par écrit, résulte d’une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d’une signification intelligible, quels que soient leur support et leurs modalités de transmission”* (yang dimaksud dengan alat bukti dengan huruf,

atau alat bukti tertulis adalah urut-urutan dari huruf-huruf, tanda-tanda, angka-angka, atau semua tanda-tanda atau simbol-simbol yang dapat difahami, bagaimana pun bentuk medianya, dan bagaimana pun cara transmisinya).

Dengan demikian, terlihat bahwa di mana pun tulisan itu ditulis dapat menjadi alat bukti, selama tulisan tersebut dapat dibuktikan dengan siapa tulisan itu terkait, dan keintegritasannya terjamin. Sehingga, Hakim dapat menganggap bahwa akta elektronik dan tanda tangan elektronik termasuk dalam alat bukti. Penggunaan interpretasi analogis terhadap akta elektronik dan tanda tangan elektronik menuntut Hakim untuk membekali dirinya dengan pengetahuan tentang sistem transaksi elektronik, ataupun mekanisme transaksi elektronik. Referensi-referensi berkaitan dengan alat bukti elektronik sudah mudah dijumpai, dengan semakin berkembangnya doktrin-doktrin[51] dari ahli hukum dan laporan-laporan penelitian mengenai adaptasi hukum pembuktian Indonesia terhadap teknologi informasi

Bentuk interpretasi lainnya adalah interpretasi ekstensif (*extensieve uitleg*), yaitu memberikan suatu penafsiran dengan memperluas arti kata-kata yang terdapat dalam ketentuan-ketentuan undang-undang tersebut, sehingga suatu peristiwa yang tidak dapat dimasukkan menjadi dapat dimasukkan. Berdasarkan metoda ini, makna “tertulis” dalam hukum acara perdata dapat diperluas seperti yang diungkapkan oleh Pitlo di atas.

Menurut Ter Haar, seorang Hakim harus mencari *maatschappelijke werkelijjkheid* (realitas kemasyarakatan), oleh karenanya penafsiran undang-undang menurut bahasa harus diakhiri dengan penafsiran sosiologis agar sebuah keputusan Hakim itu sesuai dengan realitas masyakarat[53]. Hukum pembuktian dalam acara perdata yang digunakan saat ini sudah berumur lebih dari satu abad. Sehingga seperti yang dikatakan oleh, E. Utrecht dan Moh. Saleh Djindang, *de positiviteit dekt niet meer de realiteit* (positivitas tidak lagi meliputi realitas). Di jaman ini, pendapat dari Montesquieu bahwa Hakim adalah *la bouche quiprononce les paroles de la loi* (corongnya undang-undang) sudah tidak dapat diterima lagi baik di lingkungan hukum perdata maupun pidana.

Sehingga seorang Hakim harus mencari tujuan sosial baru dari hukum pembuktian, dengan menggali, mengikuti, dan memahami nilai-nilai hukum yang hidup dalam masyarakat[54] saat ini. Penafsiran sosiologis sesungguhnya merupakan suatu alat

untuk menyelesaikan perbedaan-perbedaan antara positivitas hukum dan realitas hukum. Dengan metoda penafsiran sosiologis ini, Hakim dapat menafsirkan maksud dari hukum pembuktian tahun 1848 dari sudut pandang hukum pembuktian di abad 21. Dengan demikian, hukum akan tetap dinamis dan mampu mengikuti perkembangan jaman.

Saran terakhir dari Penulis kepada para pengguna akta elektronik dan tanda tangan elektronik dalam bertransaksi melalui jaringan *digital* yaitu memuat sebuah klausula khusus dalam kontrak yang menentukan bahwa para pihak yang terikat pada perjanjian tersebut menyatakan kesepakatannya untuk menerima akta elektronik dan tanda tangan elektronik sebagai alat bukti tertulis yang sah. Klausula ini dimungkinkan dengan berpijak pada asas kebebasan berkontrak, di mana para pihak pada asasnya dapat membuat perjanjian dengan isi yang bagaimana pun juga, asalkan tidak bertentangan dengan peraturan perundang-undangan yang berlaku dan yang bersifat memaksa (*dwigned recht*).

Pada asasnya hukum perjanjian dalam hukum perdata merupakan hukum pelengkap (*aanvullendrecht*), artinya bahwa para pihak dapat membuat suatu perjanjian yang menyimpang dari ketentuan-ketentuan undang-undang tentang hukum perjanjian, kecuali beberapa sifat yang memaksa, seperti yang ditentukan oleh Pasal 1338 KUHPerdata, "Semua perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya" (*pacta sunt servanda*). Dengan demikian, para pihak dapat bersepakat dan menetapkan bahwa akta elektronik atau tanda tangan elektronik yang digunakan dalam bertransaksi digunakan sebagai alat bukti sah, dan perjanjian ini mengikat para pihak dan mempunyai kekuatan hukum seperti halnya undang-undang.

Pencantuman klausula khusus mengenai "pembuktian dengan alat bukti elektronik" telah banyak diterapkan oleh pelaku bisnis terutama sektor perbankan yang menggunakan *internet system banking*. Salah satunya adalah *Internet Banking* Bank Central Asia (selanjutnya disingkat BCA) yang mencantumkan sebuah klausula tentang "pembuktian" yang menentukan bahwa, "(1) setiap instruksi transaksi finansial dari Nasabah yang tersimpan pada pusat data BCA dalam bentuk apapun, termasuk namun tidak terbatas pada catatan, *tape/cartridge*, *print out* komputer, komunikasi yang ditransmisi secara elektronik antara BCA dan Nasabah, merupakan alat bukti yang sah, kecuali Nasabah dapat membuktikan

sebaliknya. (2) Nasabah menyetujui semua komunikasi dan instruksi dari Nasabah yang diterima oleh BCA merupakan alat bukti yang sah meskipun tidak dibuat dokumen tertulis ataupun dikeluarkan dokumen yang ditandatangani".

Pembuktian tanda tangan elektronik

Asas praduga kehandalan (*presomption de fiabilité*)

Sebuah tanda tangan elektronik yang menggunakan prosedur yang handal layak untuk menikmati asas *presomption de fiabilité* yang kelak akan diatur dalam RUU ITE beserta Peraturan Pemerintah tentang tanda tangan elektronik. Peraturan perundang-undangan Perancis tentang tanda tangan elektronik melekatkan asas ini bila tanda tangan elektronik *securisée* (terkualifikasi) tersebut menggunakan teknik kriptologi sesuai dengan kondisi-kondisi yang ditetapkan oleh dekrit dan menggunakan sertifikat elektronik terkualifikasi yang diterbitkan oleh penyelenggara sertifikasi tanda tangan elektronik terakreditasi pemerintah.

Konflik pembuktian tanda tangan elektronik

Seandainya RUU ITE beserta perangkat pelaksanaannya sudah menjadi hukum positif maka kesulitan Hakim dalam melakukan verifikasi terhadap kehandalan sebuah tanda tangan mungkin akan tereduksi, tetapi realitas mengatakan lain. Jadi untuk saat ini, bagaimana seorang Hakim mampu memverifikasi dan memberikan nilai hukum terhadap kehandalan sebuah tanda tangan elektronik yang digunakan para pihak yang bersengketa ?

Selain seorang Hakim harus melengkapi dirinya dengan pengetahuan berkaitan dengan akta elektronik, tanda tangan elektronik dan cara kerja transaksi elektronik, dia juga dapat meminta pertolongan seorang ahli yang memiliki keahlian khusus di bidang teknologi informasi yang dapat dipertanggungjawabkan secara akademis mengenai pengetahuannya tersebut. Pada hakekatnya "alat" ini merupakan sarana bagi Hakim untuk mencari kebenaran yang hakiki agar dapat menjatuhkan keputusan yang adil. Namun, harus diperhatikan bahwa seorang Hakim tidak terikat untuk mengikuti keterangan tersebut bila berlawanan dengan keyakinannya.

Hukum pembuktian dalam hukum perdata berdasarkan Pasal 1865 KUHPerdata dan Pasal 163 HIR memuat asas "*actori incombit probatio*", artinya siapa yang mendalilkan sesuatu dia harus membuktikannya. Sepintas lalu, asas ini sangat mudah diaplikasikan di mana beban pembuktian "selalu" berada pada penggugat.

Sesungguhnya dalam praktek, Hakim sering kali kesulitan dalam menjalankan perintah Pasal ini sebab pada dasarnya tidaklah seorang pihak saja yang diwajibkan memberikan bukti, melainkan harus ditinjau dari kasus per kasus, sesungguhnya keadaan yang nyata, menurut Retnowulan Sutantio, "pembuktian itu hendaknya diwajibkan kepada pihak yang sedikit diberatkan".

Selanjutnya menurut Profesor R. Subekti, S.H. dalam bukunya "Hukum Pembuktian" mengatakan bahwa, "beban pembuktian harus dilakukan dengan adil dan tidak berat sebelah, karena suatu pembagian beban pembuktian yang berat sebelah berarti *a priori* menjerumuskan pihak yang mendapat beban terlalu berat kedalam jurang kekalahan". Berkaitan dengan beban pembuktian terhadap tanda tangan elektronik, hendaknya dibebankan kepada pihak yang mempunyai alat-alat yang memadai untuk membuktikan bahwa tanda tangan elektronik tersebut dibuat dengan prosedur yang handal dan dapat dipertanggungjawabkan.

Tanggung jawab Penyelenggara Sertifikasi Tanda Tangan Elektronik

Seperti telah diutarakan pada tulisan-tulisan sebelumnya bahwa penyelenggara sertifikasi tanda tangan elektronik (selanjutnya disingkat PSE) merupakan salah satu pemain kunci dalam sistem tanda tangan elektronik. Dialah yang menerbitkan sertifikat elektronik yang ditujukan untuk mengidentifikasi secara sempurna subyek hukum yang menandatangani secara elektronis sebuah akta elektronik. Selain itu, PSE juga menawarkan jasa pembuatan tanda tangan elektronik dengan penggunaan sebuah prosedur yang handal untuk menjaminhubungan hukum antara Penandatangan dengan akta elektronik dan integritas dari akta elektronik tersebut.

Sebelum membahas tanggung jawab PSE maka akan diuraikan terlebih dahulu secara singkat tanggung jawab dari Pengguna tanda tangan elektronik, baik yang diatur oleh RUU ITE maupun yang menjadi kebiasaan dalam transaksi elektronik, yaitu : (1) Pengguna harus memberikan pengamanan yang selayaknya atas tanda tangan elektronik yang digunakannnya, pelanggaran dari ketentuan ini akan mengakibatkan tanda tangan elektronik tersebut tidak dapat digunakan sebagai alat bukti; (2) Pengguna harus waspada terhadap penggunaan tidak sah dari data pembuatan tanda tangan oleh orang lain (kewajiban kewaspadaan); (3) Pengguna tanpa menunda-nunda, harus memberitahukan kepada PSE bila tanda tangan elektroniknya dicurigai telah dibobol oleh pihak yang tidak berkepentingan, sehingga PSE akan memblokir sertifikat elektronik terkait dan mempublikasikan ke

Certification Revocation List; dan (4) Pengguna dilarang menggunakan kunci privat untuk mengambil tindakan-tindakan yang bertentangan dengan undang-undang, kesusilaan dan ketertiban umum.

Tanggung jawab PSE baik dengan Pengguna jasanya (Penandatangan) maupun terhadap pihak ketiga dapat dituntut berdasarkan ketentuan-ketentuan yang terdapat dalam buku ke-3 KUHPerdata, yaitu tuntutan ganti rugi atas dasar *wanprestatie*/cidera janjivdan tuntutan ganti rugi atas dasar *onrechtsmatige daad*

Landasan dari tanggung jawab kontraktual

PSE mengeluarkan sertifikat elektronik yang bertujuan untuk mengidentifikasi subyek hukum/Penandatangan elektronis dan mengotentifikasi tanda tangan elektronik tersebut. Sesungguhnya, proses pemberian sertifikasi tersebut diawali dengan kesepakatan (*overeensteming*) antara pengguna dan PSE yang tertuang dalam suatu perjanjian (*overeenkomst*). Adapun asas-asas utama dari hukum perikatan yang termuat dalam buku ke-3 KUHPerdata, yaitu : (1) asas kebebasan berkontrak (*liberté contractuelle*), (2) asas konsensual (*consensualisme*), (3) asas *obligatoire* dan (4) asas *pacta sunt servand*.

Kewajiban-kewajiban yang umumnya harus dipenuhi oleh PSE ebagaimana yang dituangkan dalam perjanjian antara PSE dan pengguna jasa, sebagai berikut :

(a) PSE harus memastikan keterkaitan suatu tanda tangan elektronik dengan Penandatangan;
(b) Menggunakan sistem yang aman dan handal dalam proses pensertifikasian;
(c) Memastikan sertifikat elektronik dari Pengguna jasa yang telah disahkan. Demi keuntungan dari para Pengguna jasa, sertifikat tersebut dimuat kedalam Certificate Revocation List;
(d) Memastikan pencabutan atau pembekuan sementara sertifikat elektronik, atas persetujuan dari Pemiliknya;
(e) Memastikan secara presisi waktu diterbitkannya dan dicabutnya sebuah sertifikat elektronik;
(f) Memperkerjakan para pegawai yang mempunyai pengetahuan, pengalaman dan kualifikasi teknis yang tepat dalam proses pensertifikasian;

(g) Menggunakan sistem-sistem dan produk-produk yang menjamin keamanan teknik dari sertifikat elektronik dan kriptologi;

(h) Mengambil semua tindakan yang perlu untuk mencegah pemalsuan sertifikatelektronik;

(i) Bila PSE sebagai pembuat tanda tangan elektronik dari pengguna jasanya, PSE wajib untuk menjaga kerahasiaan dari data-data yang timbul dari proses pembuatan tersebut dan PSE harus menolak baik untuk menyimpan maupun memproduksi ulang data-data ini;

(j) Semua informasi-informasi yang terkait dengan sertifikat elektronik harus disimpan secara aman dan terjamin keintegritasannya guna menjadi alat bukti di muka pengadilan;

(k) Menggunakan sistem pengarsipan sertifikat-sertifikat elektronik yang handal dan yang menjamin :i. Pemasukan dan modifikasi terhadap data-data hanya dilakukan oleh pihak-pihak yang diberikan otorisasi oleh PSE; ii. Akses publik terhadap sertifikat elektronik hanya diijinkan bilaPemegang sertifikat memberikan persetujuannya; iii. Segala perubahan terhadap sistem dapat diketahui;

(l) Memverifikasi identitas dari subyek hukum di mana sertifikat elektronik diterbitkan untuknya dengan meminta dokumen-dokumen resminya;

(m) Ketika sertifikat elektronik tersebut akan diterbitkan, PSE harus memastikan bahwa informasi-informasi yang terkait dengan sertifikat tersebut sudah tepat dan tanda tangan elektronik dari Penandatangan telah sesuai dengan data-data dari tanda tangan elektronik yang terdapat dalam sertifikat.

(n) Dikatakan wanprestatie terhadap kewajiban-kewajibannya, bila PSE melakukan salah satu dari berikut : (1) PSE sama sekali tidak berprestasi, (2) PSE salah berprestasi, dan (3) PSE terlambat berprestasi. Akibat hukumnya berdasarkan Pasal 1246 KUHPerdata, Pemegang sertifikat elektronik yang diterbitkan PSE berhak untuk menuntut penggantian kerugian yang berupa biaya-biaya, kerugian dan bunga. Namun, penggantian kerugian ini baru mulai diwajibkan, apabila PSE telah dinyatakan lalai memenuhi perjanjiannya, tetap melalaikannya, atau sesuatu yang harus diberikan atau dibuatnya, hanya dapat diberikan yang harus diberikan atau dibuatnya, hanya dapat diberikan atau dibuat dalam tenggang waktu yang telah dilampaukanny.