BAB 2

ELECTRONIC SIGNATURE DALAM *E-COMMERCE* DI SEKTOR PERBANKAN

2.1. Kerangka Pelaksanaan *Electronic Signature*

2.1.1 Unsur-Unsur Pelaksanaan *Electronic Siganature*

Sebagaimana disebutkan pada bahasan sebelumnya mengenai definisi tanda tangan elektronik, yakni tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.[59] Definisi tanda tangan elektronik tersebut mengandung beberapa unsur fundamental sebagai ukuran sebuah tanda-tangan merupakan elektronik atau bukan. Unsur-unsur tersebut antara lain, unsur informasi elektonik, terikat atau terasosiasi informasi lain, serta sebagai alat verifikasi dan autentifikasi.

Pertama, informasi elektronik. Informasi elektronik merupakan hal terpenting dalam tanda-tangan elektronik. Informasi elektronik inilah yang menjadi landasan adanya tanda tangan elektronik. Perkembangan informasi dengan menggunakan media komputer atau media lainnya menjadikan media informasi sebagai lahan baru dunia perdagangan yang kemudian dikenal dengan istilah *electronic commerce*.

Pasal 1 Angka 1 UU ITE menyebutkan bahwa informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (*EDI*), surat

[59] Pasal 1 Angka 12 Undang-Undang No.11 Tahun 2008 tentang ITE

elektronik (*electronic mail)*, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Dari definisi Informasi Elektronik di atas memuat tiga makna informasi elektronik yakni:

a. satu atau sekumpulan data elektronik;
b. informasi elektronik memiliki wujud diantaranya tulisan, suara, gambar; dan
c. informasi elektronik memiliki arti atau dapat dipahami.

Kedua, unsur terikat atau terasosiasi (integritas) informasi lain. Integritas berhubungan dengan masalah keutuhan dari suatu data yang dikirimkan. Seorang penerima pesan atau data dapat merasa yakin apakah pesan yang diterimanya sama dengan pesan yang dikirimkan. Ia dapat merasa yakin bahwa data tersebut tidak pernah dimodifikasi atau diubah selama proses pengiriman atau penyimpanan.[60]

Penggunaan *electronic signature* yang diaplikasikan pada pesan atau data elektronik yang dikirimkan dapat menjamin bahwa pesan atau data elektronik tersebut tidak mengalami suatu perubahan atau modifikasi oleh pihak yang tidak berwenang. Jaminan *authenticity* ini dapat dilihat dari adanya *hash function*[61] dalam sistem *electronic signature*, dimana penerima data (recipient) dapat melakukan pembandingan *hash value*. Apabila *hash value*-nya sama dan sesuai,

---

[60] Arrianto Mukti Wibowo, S.Kom, dkk, *Kerangka Hukum Electronic signature dalam Elektronic Commerce*, Makalah untuk Masyarakat Telekomunikasi Indonesia pada bulan Juni 1999 di Pusat Ilmu Komputer Universitas Indonesia, Depok, Jawa Barat.

[61] Suatu metode yang digunakan untuk mengubah data-data yang ada menjadi sebuah bilangan yang relatif kecil (*small number*) yang akan menjadi "sidik jari" (*fingerprint*) dari data tersebut. Fungsi ini memecah dan mengolah data untuk menghasilkan kode atau nilai hashnya. Nilai hash dari suatu fungsi hash akan memiliki panjang yang tetap untuk masukan dengan panjang yang sembarang. http://www.wikipedia.org

maka data tersebut benar-benar otentik, tidak pernah terjadi suatu tindakan yang sifatnya mengubah (modify) dari data tersebut pada saat proses pengiriman, sehingga terjamin *authenticity*-nya. Sebaliknya apabila *hash value*-nya berbeda, maka patut dicurigai dan langsung dapat disimpulkan bahwa *recipient* menerima data yang telah dimodifikasi.[62]

Unsur ini berkaitan dengan substansi dari akta yang di dalamnya dibubuhi tanda tangan elektonik. Informasi yang berada di dalam akta elektronik tersebut merupakan informasi yang terasosiasi atau terikat. Sehingga antara informasi yang tercantum dan tanda tangan yang terbubuhi merupakan kesatuan yang tidak dapat dipisahkan. Tanda tangan digital menjadi alat pengesahan akan keotentikan dari informasi yang berada di dalam akta tersebut.[63]

Ketiga, sebagai alat verifikasi dan autentifikasi. Tanda tangan elektronik merupakan alat yang sah untuk menjadi alat bukti. Dalam Pasal 10 UU ITE disebutkan bahwa tanda tangan memiliki kekuatan hukum selama memenuhi syarat yang ditentukan UU ITE. Melalui verifikasi dan autentifikasi maka data elektronik yang dikirimkan akan diketahui asal usulnya. Peran sertifikat elektronik juga ada untuk menjaga integritas pesan. Sertifikat elektronik berisikan informasi pengguna, antara lain:[64]

1. identitas;
2. kewenangan;
3. kedudukan hukum; dan

---

62 Arrianto Mukti Wibowo, S.Kom, dkk, *op.cit,* hal 11-12.
63 *Ibid*.
64 *Ibid*, hal 11-12.

4. status dari pengguna.

Untuk menentukan sebarapa besar kewenangan yang dimiliki oleh pengguna, maka sertifikat elektronik ini memiliki berbagai tingkatan. Kewenangan atau kualifikasi diperlukan jika suatu perusahaan akan melakukan perbuatan hukum. Misalnya bila suatu perusahaan akan melakukan perbutan hukum, maka sertifikat elektronik yang berlaku adalah sertifikat elektronik yang dimiliki oleh direksi karena yang dapat mewakili perusahaan adalah direksi. Sehingga selain direksi, kualifikasi atau kewenangan penggunaan sertifikat elektronik tersebut tidak dapat digunakan oleh siapapun.[65]

Selain ketiga unsur tersebut juga terdapat beberapa unsur yang walau secara uraian definisi tanda tangan elektonik tidak termasuk, namun unsur ini merupakan faktor yang mempengaruhi tanda tangan elektronik. Unsur tersebut diantaranya unsur *non-repudiation*. *Non-repudiation* merupakan aspek yang sangat penting dalam transaksi elektronik. Aspek ini seringkali dilupakan. Aspek *non-repudiation* menjamin bahwa pelaku transaksi tidak dapat mengelak atau menyangkal telah melakukan transaksi.

Dalam sistem transaksi konvensional, aspek *non-repudiation* ini diimplementasikan dengan menggunakan tanda tangan. Dalam transaksi elektronik, aspek *non-repudiation* dijamin dengan penggunaan tanda tangan elektronik *(electronic signature)*, penyediaan *audit trail* (log), dan pembuatan sistem dapat diperiksa dengan mudah (*auditable*). Implementasi mengenai hal ini sudah tersedia, hanya perlu diaktifkan dan diakui saja. Dalam UU Informasi dan

---

[65] *Ibid.*

Transaksi Elektronik tanda tangan elektonik diakui sama sahnya dengan tanda tangan konvensional.[66]

Non repudiation ini timbul dari keberadaan *electronic signature* yang menggunakan enkripsi asimetris (*asymmetric encryption*). Enkripsi asimetris ini melibatkan keberadaan dari kunci privat dan kunci publik. Pesan yang telah terenkripsi dengan kunci privat akan hanya dapat dibuka melalui kunci publik dari pengirim pesan, sehingga pengirim pesan tidak akan dapat menyangkal yang dikirimnya karena terbukti bahwa pesan tersebut dapat didekripsi dengan kunci publik pengirim. Keutuhan dari pesan tersebut dapat dilihat dari keberadaan *hash function* dari pesan tersebut, dengan catatan bahwa data yang telah di-sign akan dimasukkan kedalam *electronic envelope*.[67]

Selain unsur *non-repudiation* tanda tangan elektronik juga mengandung unsur kerahasiaan (*confidential*). *Confidentiality* merupakan aspek yang menjamin kerahasiaan data atau informasi. Sistem yang digunakan untuk mengimplementasikan transaksi elektronik melalui tanda tangan elektonik harus dapat menjamin kerahasiaan data yang dikirim, diterima dan disimpan. Kerahasiaan ini dapat diimplementasikan dengan berbagai cara, seperti misalnya menggunakan teknologi kriptografi dengan melakukan proses enkripsi (penyandian/pengkodean) pada transmisi data, pengolahan data (aplikasi dan database), dan penyimpanan data (storage). Teknologi kriptografi dapat

---

[66] Budi Rahardjo, *E-Procurement Security*, Makalah pada seminar *Sosialisasi Keppres No. 61/2004 tentang Pengadaan Barang dan Jasa Pemerintah secara elektronik dan aplikasi perpajakannya*, yang diselenggarakan oleh Lembaga Pendidikan dan Pelatihan Perpajakan, Properti dan Administrasi Bisnis Artha Bhakti, di Sahid Jaya Hotel, Jakarta, 20 April 2005,hal.2.

[67] Arrianto Mukti Wibowo, S.Kom, dkk, *op cit*, hal 11-12.

mempersulit pembacaan data tersebut bagi pihak yang tidak berhak atas informasi.[68]

Akses terhadap informasi juga harus dilakukan dengan melalui mekanisme otorisasi (*authorization*) yang ketat. Tingkat keamanan dari mekanisme otorisasi bergantung kepada tingkat kerahasiaan data yang diinginkan.

Undang-Undang ITE memberikan definisi terhadap kata "tanda tangan" yang sesungguhnya mempunyai dua fungsi hukum dasar, yaitu : (1) tanda identitas penanda tangan; dan (2) sebagai tanda persetujuan dari penanda tangan 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.[69]

Bila dikaitkan dengan UU ITE, maka UU ITE memberikan definisi lebih ke sudut teknik, padahal sebuah tanda tangan mempunyai tujuan untuk menerima atau menyetujui secara meyakinkan isi dari sebuah tulisan. Hal ini sangat logis, di mana tanda tangan elektronik mempunyai dua fungsi hukum dasar. Oleh karenanya, tanda tangan elektronik dapat didefinisikan 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.[70]

---

68 Budi Rahardjo, *op cit*, hal. 2.

69 Julias Indra Dipayaono Singgara, *Pengakuan Tanda Tangan Digital dalam Hukum Pembuktian Indonesia*, hal 3. http://www.legalitas.org

70 *Ibid*, hal.3-4.

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.

Pasal 11 ayat (1) huruf (a) sampai dengan huruf (f) UU ITE menentukan sebagai berikut:

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

Ketentuan Pasal 11 merupakan syarat minimal yang harus dipenuhi sebuah tanda tangan elektronik sebelum menikmati “asas praduga kehandalan” yang

memberikan kekuatan hukum dan akibat hukum yang sama dengan tanda tangan manuskrip.[71]

2.1.2. Ruang Lingkup Penerapan Tanda Tangan Elektronik

Tanda tangan digital yang diatur dalam Pasal 11 dan 12 UU ITE, juga telah dipersiapkan pengaturan dalam Rancangan Peraturan Pemerintah tentang Tanda Tangan Elektronik (terakhir diakulmulasi dengan manteri muatan UU ITE lainnya ke dalam RPP tentang Penyelenggaraan Informasi dan Transaksi Elektronik) yang telah dipersiapkan oleh Departemen Komunikasi dan informasi.

Ruang lingkup pelaksanaan tanda tangan elektronik adalah setiap verifikasi dan autentifikasi terhadap informasi elektronik yang diselenggarakan oleh pelaku teknologi informasi, baik di dalam Indonesia ataupun antara Indonesia dengan luar negeri, dimana tanda tangan elektronik berlaku terhadap segala jenis transaksi yang berkaitan dengan kegiatan usaha, hubungan produsen dan konsumen, atau hubungan perdagangan antara beberapa pihak.

Suatu transaksi konvensional mensyaratkan adanya dokumen yang ditandatangani sebagai bentuk autentifikasi terhadap perbuatan hukum tersebut. Tanda tangan elektronik yang diatur dalam UU ITE memperbolehkan suatu autoritas yang berwenang melakukan autentifikasi dan verifikasi terhadap dokumen elektronik yang ditandatangan secara elektrnik. Informasi elektronik yang di dalamnya terintegrasi tanda tangan elektronik serta disertifikasi melalui sertifikat elektronik yang dibuat oleh penyelenggara sertifikasi elektronik.

---

[71] *Ibid*, hal.4.

Pelaksanaan informasi elektronik, dokumen elektronik, dan autentifikasi serta verifikasi melalui tanda tangan elektronik tidak dapat dilakukan terhadap suatu kontrak yang diharuskan dalam bentuk tertulis. Pasal 5 ayat (4) dan Pasal 6 UU ITE mengecualikan informasi, dokumen, dan tanda tangan yang tidak dapat dibuat secara elektronik, yakni terhadap:

a. surat yang menurut undang-undang harus dibuat dalam bentuk tertulis;
b. surat beserta dokumennya yang menurut undang-undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta; dan
c. ketentuan lain yang menyaratkan suatu informasi harus berbentuk tertulis atau asli, informasi elektronik dan/atau dokumen elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Pelaksanaan suatu kontrak dalam bentuk elektronik, harus tetap didasarkan pada hukum kontrak yang berlaku dalam hal ketentuan-ketentuan di atas, sehingga tidak semua dokumen, tanda tangan, dan informasi harus dibuat secara elektronik. Ketentuan-ketentuan dalam hukum kontrak yang mewajibkan dibuat secara konvensional (tertulis), maka mengecualikan ketentuan dalam UU ITE.

Suatu tanda tangan elektronik dianggap sah bila dibuat hanya oleh subjek yang berwenang terhadap informasi elektronik yang disertifikasi melalui sertifikat elektronik. Subjek hukum yang tidak berwenang terhadap dokumen elektronik tersebut tidak dapat melakukan tanda tangan elektonik. Sehingga, orang atau badan hukum yang menerima tanda tangan elektronik tersebut harus memastikan

bahwa tanda tangan elektronik tersebut memang dibuat oleh subjek hukum yang memiliki kewenangan.

Apabila peraturan perundang-undangan yang berlaku menentukan terminasi terhadap suatu dokumen, maka dalam dokumen elektronik pun memiliki terminasi (bila diatur dalam dokumen elektronik), dengan ketentuan bahwa dokumen elektronik tersebut:[72]

a. merefleksikan secara akurat keterangan yang terdapat dalam kontrak atau dokumen tersebut; dan
b. dokumen elektronik tersebut tetap dapat diakses oleh setiap orang yang berwenang.

2.1.3. Proses Tanda Tangan Elektronik

Pasal 11 UU 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 12 UU 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,[73] dengan kata

---

[72] Ari Juliano Gema, *E-Sign Act: Keberlakuan dan Hambatannya,,* lihat http://onno.vlsm.org/v01/OnnoWPurbo/contrib/aplikasi/ hukum/e-sign-act-keberlakuan-dan-hambatannya-10-2000.rtf

[73] Anonymous. http://www.juriscom.net

lain kriptologi merupakan kombinasi dari kriptografi (*cryptographie*)[74] dan kriptanalis(*cryptanalyse*).[75]

Teknik kriptologi bukanlah sebuah teknik baru, ia telah digunakan sejak jaman Julius Cesar, tetapi pada masa sekarang, 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.[76] Berkaitan dengan keamanan pesan rahasia, teknik kriptologi modern menjamin sedikitnya lima keamanan minimal, yaitu:[77]

a. keotentikan penerima pesan harus mengetahui siapa pengirim pesan tersebut dan harus benar-benar yakin bahwa pesan tersebut berasal dari pengirim;
b. integritas penerima harus yakin bahwa pesan tersebut tidak pernah diubah, atau dipalsukan oleh pihak beritikad tidak baik;
c. kerahasiaan pesan tersebut harus tidak dapat dibaca oleh pihak yang tidak berkepentingan;
d. tidak dapat disangkal, pengirim tidak dapat menyangkal bahwa bukan dia yang mengirim pesan tersebut; dan
e. kontrol akses sistem kriptologi mempunyai kemampuan untuk memberikan otorisasi ataupun melarang atas setiap akses ke pesan-pesan tersebut.

---

74 *Ibid*

75 Ilmu yang menganalisa bagaimana memecahkan sebuah tulisan/dokumen terenkripsi menjadi jelas atau dapat diketahui isinya tanpa mengetahui kunci rahasia yang digunakan dalam proses enkripsi. *An introduction to cryptographie,* Juni 2004, hal. 71.

76 www.juriscom.net, *op.cit*,hal.4.

77 *Ibid*,hal.16.

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

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.[78] 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. Berkat algoritma ini, Phil Zimmerman mampu membuat sebuah piranti lunak yang diberi nama *Pretty Good Privacy*[79] (selanjutnya disebut PGP).[80]

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

---

78 *Ibid*,hal.16.
79 Salah satu software pengaman kriptografi yang cukup tinggi performansinya.
80 Lihat http://www.pgpi.org/products/pgp/versions/freeware/, hal.2.

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.[81]

Semakin panjang kunci tersebut (semakin besar "bit" dari kunci) maka akan semakin sulit untuk membobol kunci kriptologi. Di Indonesia, panjang kunci ini dapat dibuat sebebas-bebasnya. Namun, kunci privat harus disimpan dan dijaga kerahasiaannya. Teknik kriptologi asimetris ini merupakan dasar dari pembuatan tanda tangan elektronik.

Untuk menandatangani secara elektronik sebuah pesan, dengan bantuan piranti lunak, pengirim akan membuat pertama-tama sebuah *message digest*[82] dari pesan yang asli dengan menggunakan *hash function*. *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 pengirim maupun penerima dapat mengetahui keintegritasan pesan tersebut.[83]

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

---

81 *Ibid.*

82 Merupakan "DNA" dari pesan asli. bila terjadi perubahan satu karakter saja maka "DNA" nya akan berubah, dengan kata lain, satu pesan akan mempunyai satu "DNA" unik.

83 http://www.pgpi.org/products/pgp/versions/freeware/, *op.cit* 3.

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 diubah Sekalipun begitu, proses ini tidak dapat mengotentifikasi identitas penulis pesan tersebut.[84]

Adapun proses teknis dalam pembuatan tanda tangan elektronik sebagaimana dijelaskan di atas, maka sebelum tanda tangan elektronik digunakan maka penyelenggara tanda tangan elektronik wajib memastikan identifikasi awal penanda tangan dengan cara sebagai berikut:[85]

a. penanda tangan menyampaikan identitas kepada penyelenggara tanda tangan elektronik;
b. penanda tangan melakukan registrasi kepada penyelanggara atau pendukung penanda tangan elektronik sebelum menggunakan tanda tangan elektronik dalam suatu transaksi elektronik;
c. dalam hal diperlukan, penyelenggara tanda tangan elektronik dapat melimpahkan secara rahasia data identitas penanda tangan kepada penyelenggara pendukung layanan data tanda tangan elektonik lain dengan cara persetujuan penanda tangan.

---

84 Julius Singara, *op.cit,* hal. 80

85 Pasal 14 ayat (1) RPP tentang Penyelenggarakan Informasi dan Transaksi Elekronik (RPP PITE)

Mekanisme yang digunakan oleh penyelenggara tanda tangan elektronik untuk pembuktian identitas penanda tangan secara elektronik wajib menerapkan kombinasi paling kurang dua faktor autentifikasi.[86]

Faktor autentifikasi yang dapat dipiih untuk dikombinasikan, terdiri dari tiga, yakni:

a. sesuatu yang dimiliki secara individu (*what you have*), misalnya kartu ATM atau *smart Card*;
b. sesuatu yang diketahui secara individu (*what you know*), misalnya *password*, PIN, atau kunci kriptografi; dan
c. sesuatu yang merupakan ciri/karakteristik seorang individu (*what you are*), misalnya pola suara (*voice pattern*), dinamika tulisan tangan (*handwriting dynamic*), sidik jari (*finggerprint*), dan lain-lain.

2.2. Electronic Commerce dan Secure Elecrtonic Transaction di Sektor Perbankan

2.2.1. Bentuk-bentuk E-commerce di Sektor Perbankan

Perkembangan ilmu pengetahuan dan teknologi mengakibatkan berbagai perubahan kinerja manusia dalam perdagangan, termasuk perdagangan elektronik di sektor perbankan melalui media elektronik.

Salah satu bentuk media yang terus terinovasi yakni media komputer yang mampu terkoneksi telekomunikasi berupa media internet, suatu koneksi antar jaringan komputer secara cepat. Perkembangan perdagangan ini sejalan dengan

[86] Pasal 14 ayat (3) RPP PITE.

apa yang diprediksikan oleh Alvin Toffler dalam bukunya *The Third Wave* bahwa di era millennium ketiga, teknologi akan memegang peranan yang signifikan dalam kehidupan manusia.[87]

Aplikasi dibidang bisnis yang menggunakan koneksi komputer dan internet, dalam hal ini perdagangan, yaitu *e-commerce*. *E-commerce* sebagai bagian dari *e-business*, oleh para ahli dan pelaku bisnis coba didefinisikan sebagai segala bentuk transaksi perdagangan atau perniagaan barang atau jasa (*trade of goods and services*) dengan menggunakan media elektronik.[88]

E-commerce terjadi dalam berbagai macam perdagangan yang ada, mulai dari perdagangan barang ataupun jasa. Perdagangan jasa yang seringkali digunakan oleh perusahaan dan perorangan adalah perdagangan jasa perbankan. Bank sebagai badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak[89] dalam menjalankan usahanya kini telah menggunakan pelayanan berbasis elekronik selain pelayanan manual yang telah ada.

Era teknologi informasi dewasa ini berimplikasi adanya upaya dari perusahaan pebankan untuk terus meningkatkan pelayanan kepada nasabah agar perkembangan teknologi informasi mampu diikuti dengan responsif demi pelayanan prima kepada nasabah melalui transaksi yang cepat dan mudah.

---

87 Alvin Toffler, *The Third Wave*. http://www.skypoint.com/members/mfinley/toffler.htm
88 Novia Iman, *Mengenal E-commerce*, www.noviaiman.com.
89 Pasal 1 Angka 2 UU No. 10 Tahun 1998 tentang Perbakan.

E-commerce perbankan digunakan sebagai transaksi bisnis antara perusahaan yang satu dengan perusahaan yang lain, antara perusahaan dengan nasabah, atau antara perusahaan dengan institusi yang bergerak dalam pelayanan publik. Jika diklarifikasikan, sistem *e-commerce* di sektor perbankan terbagi menjadi tiga tipe aplikasi, *yaitu electonic markets, electronic data interchange, dan internet commerce*.[90]

2.2.1.1. *Electronic Markets* (EMs)

EMs adalah sebuah sarana yang menggunakan teknologi informasi dan komunikasi untuk melakukan penawaran dalam sebuah segmen pasar, sehingga pembeli dapat membandingkan berbagai macam harga yang ditawarkan. Dalam pengertian lain, EMs adalah sebuah sistem informasi antar organisasi yang menyediakan fasilitas-fasilitas bagi para penjual dan pembeli untuk bertukar informasi tentang harga dan produk yang ditawarkan. Keuntungan fasilitas EMs bagi pelanggan adalah terlihat lebih nyata dan efisien dalam hal waktu, sedang bagi penjual, ia dapat mendistribusikan informasi mengenai produk dan *service* yang ditawarkan dengan lebih cepat sehingga dapat menarik pelanggan lebih banyak.

2.2.1.2. *Electronic Data Interchange* (EDI)

EDI adalah sarana untuk mengefisienkan pertukaran data transaksi-transaksi regular yang berulang dalam jumlah besar antara organisasi-organisasi komersial. Secara formal EDI didefinisikan oleh *International Data Exchange*

---

[90] Sakti, Nufransa Wira, *Perpajakan dalam E-Commerce, Belajar dari Jepang*, dalam Berita Pajak No.1443/Tahun XXXIII/15 Mei 2001, hal.35

Assosiation (IDEA) sebagai "transfer data yang terstruktur dengan format standard yang telah disetujui yang dilakukan dari satu sistem komputer ke sistem komputer yang lain dengan menggunakan media elektronik". Keuntungan dalam menggunakan EDI adalah waktu pemesanan yang singkat, mengurangi biaya, mengurangi kesalahan, memperoleh respon yang cepat, pengiriman faktur yang cepat dan akurat serta pembayaran dapat dilakukan secara elektronik.

2.2.1.3. *Internet Commerce.*

Internet commerce adalah penggunaan internet yang berbasis teknologi informasi dan komunikasi untuk perdagangan. Kegiatan komersial ini seperti iklan dalam penjualan produk dan jasa. Transaksi yang dapat dilakukan di internet, antara lain, dalam penjualan produk dan jasa. Transaksi yang dapat dilakukan di internet antara lain pemesanan atau pembelian barang dimana barang akan dikirim melalui pos atau sarana lain setelah uang ditransfer ke rekening penjual. Keuntungan dari penggunaan internet sebagai media pemasaran dan saluran penjualan adalah untuk beberapa produk tertentu lebih sesuai ditawarkan melalui internet; harga lebih murah mengingat membuat situs di internet lebih murah dibandingkan dengan membuka outlet retail di berbagai tempat; internet merupakan media promosi perusahaan dan produk yang paling tepat dengan harga yang relatif lebih murah; serta pembelian melalui internet akan diikuti dengan layanan pengantaran barang samapi ditempat pembeli.

E-commerce di sektor perbankan sebagai bentuk perdagangan dalam prakteknya, memiliki beberapa karakteristik. Karakteristik *e-commerce* diantaranya[91]:

a. transaksi tanpa batas; bahwa transaksi tidak lagi dibatasi oleh waktu dan letak geogerafis.
b. transaksi anonim; bahwa penjual dan pembeli dalam transaksi tidak harus bertemu.
c. produk digital dan nondigital; bahwa produk-produk digital dapat dipasarkan melalui internet dengan cara mendownload secara elektronik.
d. produk barang tak berwujud; dapat menawarkan barang tak berwujud seperti transaksi keuangan untuk pembayaran.

E-commerce pada sektor perbankan dapat diklarifikasikan menjadi dua jenis yaitu: *business to business* (b2b) dan *business to customer* (b2c). *Business to business* adalah sistem komunikasi bisnis online antar pelaku bisnis (perbankan bekerja sama dengan perusahaan lain dengan menggunakan EDI), sedangkan *business to customer* merupakan mekanisme servis online kepada nasabah (transaksi melalaui internet *banking*), yaitu transaksi antara bank dengan *customer*. Dalam *business to business* pada umumnya transaksi dilakukan oleh para pelaku yang sudah saling kenal dengan format data yang telah disepakati bersama. Sedangkan dalam *business to customer* sifatnya terbuka untuk publik, sehingga setiap individu dapat mengaksesnya melalui suatu *web server*.

---

91 *Ibid*, hal 35.

Transaksi elektronik antara para pelaku bisnis maupun nasabah dalam menggunakan jasa perbankan yang terjadi di dunia maya dilakukan melalui *paperless transaction*, yakni transaksi yang tidak berbasis dokumen berwujud (*paper document*) melainkan menggunakan sistem *digital document*.

Transaksi berbasis *digital document* tersebut dilaksanakan melalui kontrak online, yang menurut Santiago Canavillas dan A. Martines Nadal, sebagaimana dikutip oleh Aryad Sanusi memiliki banyak tipe dan variasi, yaitu:[92]

a. Kontrak melalui *chating* dan *video conference*;

Kontrak ini dilakukan melalui media komunikasi yang disediakan oleh internet melalui dialog interaktif secara langsung antara penyedia jasa perbankan dengan nasabah. Dengan *chating* seseorang dapat berkomunikasi secara langsung, tapi hanya dapat dilakukan melalui tulisan atau pernyataan yang terbaca pada komputer masing-masing. Sedangkan *video conference* adalah alat untuk berbicara dengan beberapa pihak dengan melihat gambar dan mendengar suara secara langsung pihak yang dihubungi dengan alat ini. Dengan demikian melakukan kontrak dengan menggunakan jasa *chating* dan *video conference* ini dapat dilakukan secara langsung antara beberapa pihak dengan menggunakan sarana komputer atau nomor monitor televisi.

b. Kontrak melalui e-mail;

---

92 Sanusi, Arsyad, *E-Commerce, Hukum dan Solusinya*, PT Mizan Grafikas, Jakarta, 2001, hal.64.

Kontrak online melalui e-mail merupakan kontrak yang sangat populer dan mendunia dengan biaya yang sangat murah dan waktu yang efisien. Untuk mendapatkan alamat e-mail dapat dilakukan dengan mendaftarkan diri kepada penyedia layanan e-mail gratis atau dengan mendaftarkan diri sebagai *subscriber* pada *server* atau ISP tertentu. Kontrak e-mail dapat berupa penawaran yang dikirimkan kepada nasabah. Di samping e-mail dapat dilakukan transaksi melalui *situs web* yang memposting permintaan nasabah, sedangkan konfirmasi melalui e-mail.

c. Kontrak melalui web atau situs.

Kontrak melalui *web* atau situs dapat dilakukan dengan cara situs *web* seorang *supplier* (baik yag berlokasi di *server supplier* maupun diletakkan pada *server* pihak ketiga) memiliki deskripsi produk atau jasa dan satu seri halaman yang bersifat *self-contraction,* yaitu dapat digunakan untuk membuat kontrak sendiri, yang memungkinkan pengunjung web untuk memesan jasa perbankan tersebut. Para nasabah harus menyediakan informasi personal dan harus menyertakan nomor kartu produk perbankan yang tersedia (*credit card,* ATM,dll).

Dunia perbankan mengenal istilah *electronic banking* dalam praktek e-commerce. Bank menyediakan layanan *electronic banking* atau *e-banking* untuk memenuhi kebutuhan *customers*, media ini merupakan media yang digunakan selain media *Automatic Teller Machine* (ATM). *E-banking* mempermudah *customers* dalam melakukan transaksi, karene *e-banking* dapat dilakukan dimanapun dan kapanpun melalui jaringan elektronik, seperti internet, *handphone*, telepon, sehingga tanpa harus menunggu di teller atau ATM.

E-banking terdiri dari layanan *internet banking, mobile banking, phone banking, dan sms banking.*

a. *Internet banking*

Internet banking adalah transaksi perbankan, baik finansial maupun nonfinansial, yang dilakukan melalui media komputer yang terhubung dengan jaringan internet bank. Jenis transaksi yang dapat dilakukan melalui *internet banking* berupa transaksi dana, informasi saldo, mutasi rekening, informasi nilai tukar, pembayaran tagihan (misalnya kartu kredit, telepon, *handphone*, listrik, PAM, dan lain-lain). Pembelian (misalnya pembelian isi ulang, tiket pesawat, saham, dan lain-lain).

Sebagai upaya *secure electronic transaction* ada beberapa hal yang perlu diperhatikan untuk keamanan transaksi *internet banking*:[93]

a). jangan pernah memberitahukan *user* ID dan *Personal Identification Number* (PIN) kepada orang lain, termasuk perugas dan karyawan bank.

b). jangan meminjamkan *Key Token* pengaman transaksi kepada orang lain.

c). jangan mencatat *user* ID di tempat yang mudah diketahui orang lain.

d). gunakan *user* ID dan PIN secara berhati-hati agar tidak terlihat dan diketahui orang lain.

e). pastikan akses alamat situs bank dengan benar.

b. Mobile Banking

Mobile banking adalah layanan perbankan yang dapat diakses langsung melalui telepon selular/*handphone* GSM (*Global for Mobile Communication*) dengan menggunakan SMS (*Short Message Service*). Jenis transaksi yang dapat

[93] Lihat www.bi.go.id

dilakukan melalui *mobil banking* berupa transfer dana, informasi saldo, mutasi rekening, informasi nilai tukar, pembayaran (kartu kredit, PLN, telepon, *handphone*, listrik, asuransi, dan lain-lain), pembelian (pulsa isi ulang, saham).

Secure electronic transaction dalam *mobile banking* dapat dilakukan dengan[94]:

a). pengamanan terhadap PIN *mobile banking*.

b). membuat PIN baru, jika merasa diketahui orang lain.

c). bila SIM Card GSM hilang, dicuri, atau dipindahtangankan kepada pihak lain, segara memberitahukan ke bank.

c. *Phone Banking*

Phone banking adalah layanan yang diberikan untuk kemudahan dalam mendapatkan infromasi perbankan dan kemudahan melakukan transaksi finansial *non-cash* melalui telepon.

d. *SMS Banking*

SMS Banking adalah layanan informasi perbankan yang dapat diakses langsung melalui telepon selular/*handphone* dengan menggunakan media SMS (*Short Massage Service*).

e. *Electronic Fund Transfer* (EFT)

EFT diartikan sebagai segela jenis transaksi yang dilakukan selain menggunakan instrumen cek, draft, atau instrumen lainnya yang dilakukan melalui terminal, instrumen telepon, komputer, atau *magnetic tape* untuk memberikan arahan, instruksi, perintah, atau wewenang kepada isntitusi keuangan

[94] *Ibid.*

(bank, credit union) untuk melakukan pendebetan atau pengkreditan terhadap suatu rekening.[95] Bentuk *electronic bangking* ini dapat dilakukan melalui media ATM, *sms banking, mobile banking, internet banking, dan phone banking*.

2.2.2. *Secure Electronic Transaction*

Secure Electronic Transaction (SET) adalah sebuah protokol komunikasi perdagangan elektronik di Internet. Protokol ini menawarkan keamanan transaksi pembayaran dengan memanfaatkan sertifikat digital untuk menjamin autentikasi, kerahasiaan, dan integritas data transaksi yang dikirimkan melalui internet. Protokol SET mengatur bagaimana *cardholder* (pemakai kartu kartu pembayaran) mendapatkan sertifikat elektronik untuk melakukan transaksi dalam SET. Dalam spesifikasi SET diterangkan bagaimana *cardholder* menghubungi *cerfificate authority* (CA) untuk mendapatkan sertifikat elektronik.[96]

Perdagangan elektronik saat ini berkembang sangat pesat didunia termasuk di Asia. Seiring dengan meningkatnya perdagangan elektronik khususnya di internet, meningkat pula jumlah pengguna kartu pembayaran sebagai alat pembayaran yang paling praktis di internet. Peningkatan tersebut diikuti pula dengan peningkatan jumlah penipuan dan kejahatan di internet. *Secure electronic transaction* (SET) adalah sebuah protokol yang khusus dibangun untuk menangani keamanan transaksi kartu pembayaran di internet. SET menjamin keaslian, kerahasiaan, dan keutuhan data transaksi yang dikirim melalui internet. Protokol SET mengatur bagaimana *cardholder* (pemakai kartu pembayaran) dan

---

[95] Buletin Hukum Perbankan dan Kebanksentralan Volume 3 Nomor 2, *Sekilas Pengatutan Electronic Banking dan electronic Fund Transfer di Amerika Serikat*, 2005, Bank Indonesia.

[96] Haris, *Implementasi Prototipe Proses Permintaan Sertifikat X.509 pada Protokol Secure Electronic Transaction*. http://vlsm.org/fusilkom-ui/fusilkom-99-s199abs.html , hal 1.

merchant (pedagang) bertansaksi, mengatur bagaimana *merchant* dan *payment gateway* (gerbang pembayaran) melakukan otorisasi kartu pembayaran dan permintaan pembayaran, mengatur bagaimana setiap pihak yang terlibat memiliki suatu sertifikat digital sebagai jaminan atas dirinya.[97]

Bentuk dari *secure electronic transaction* dalam meningkatkan keamanan dengan menggunakan teknologi kriftografi, yaitu dengan menggunakan enskripsi untuk mengacak data. Salah satu metode yang mulai umum digunakan adalah pengaman informasi dengan menggunakan *public key system*. Sistem lain yang digunakan juga adalah *privat key system*. Infrastuktur yang dibentuk oleh sistem *public key* ini disebut *public key infrastucture* (PKI), dimana kunci publik dapat dikelola untuk pengguna yang tersebar (di seluruh dunia), bentuk-bentuk komponen ini diantaranya *certification authority (CA), internet protocol security* (IPSec), *pretty good privacy (PGP), privacy enhanced mail (PEM), public key cryptography standards (PKCS), secure/multipurpose internet mail extensions (S/MIME), secure sockets layer (SSL),* dan *transport layer security (TLS v1)*:[98]

2.2.2.1 *Certification Authority* (CA)

Merupakan sebuah *body/entity* yang memberikan dan mengelolah sertifikat elektronik yang dibutuhkan dalam transaksi elektronik. CA berhubungan erat dengan pengelolaan *public key system*. CA dalam undang-undang ITE dikenal dengan istilah Penyelenggara Sertifikasi Elektronik (PSE), yakni badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik.

---

97 Haris, *ibid*, hal.2.

98 Budi Rahardjo, *Mengimplementasikan Electronic Commerce di Indonesia*, PPAU Mikroelektronika ITB, hal-6-7.

CA atau PSE dalam penyelenggaraannya dapat dilakukan oleh PSE Indonesia atau asing dengan berbadan hukum dan domisili Indonesia. PSE/CA ini erat kaitannya dengan sertifikat elektronik yang di dalamnya tercantum tanda tangan elektronik. sehingga CA/PSA harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, yang meliputi[99]:

a) metode yang digunakan untuk mengidentifikasi penanda tangan;
b) hal yang dapat digunakan untuk mengetahui data diri pembuat tanda tangan elektronik; dan
c) hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan tanda tangan elektronik.

2.2.2.2. *Internet Protocol Security (IPSec)*

IPSec adalah sebuah protokol yang digunakan untuk mengamankan transmisi *datagram* dalam sebuah *internetwork* berbasis TCP/IP.[100] IPSec mendefiniskan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (*internetwork layer*).[101] IPSec melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik tunneling untuk mengirimkan informasi melalui

---

99 Pasal 14 huruf a sampai dengan huruf c, UU No.11 Tahun 2008 tentang ITE.

100 TCP/IP (singkatan dari *Transmission Control Protocol*/*Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (software) di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP stack

101 *DARPA Reference Mode* adalah sebuah referensi protokol jaringan yang digunakan oleh protokol TCP/IP yang dibuat oleh DARPA. Model referensi ini mirip dengan OSI Reference Model, di mana setiap lapisan yang ada di bawah menyediakan layanan untuk lapisan yang berada di atasnya, dan lapisan yang ada di atas menggunakan layanan untuk lapisan yang ada di bawahnya.

jaringan Internet atau dalam jaringan Intranet secara aman. IPSec didefinisikan oleh badan *Internet Engineering Task Force* (IETF) dan diimplementasikan di dalam banyak sistem operasi. Windows 2000 adalah sistem operasi pertama dari Microsoft yang mendukung IPSec.[102]

Dalam sistem operasi Windows 2000, Windows XP, dan Windows Server 2003, kebijakan keamanan tersebut dibuat dan ditetapkan pada level *domain Active Directory* atau pada *host* individual dengan menggunakan *snap-in* IPSec *Management* dalam *Microsoft Management Console* (MMC). Kebijakan IPSec tersebut, berisi beberapa peraturan yang menentukan kebutuhan keamanan untuk beberapa bentuk komunikasi. Peraturan-peraturan tersebut digunakan ntuk memulai dan mengontrol komunikasi yang aman berdasarkan sifat lalu lintas IP, sumber lalu lintas tersebut dan tujuannya. Peraturan-peraturan tersebut dapat menentukan metode-metode autentikasi dan negosiasi, atribut proses *tunneling*, dan jenis koneksi.[103]

Untuk membuat sebuah sesi komunikasi yang aman antara dua komputer dengan menggunakan IPSec, maka dibutuhkan sebuah *framework* protokol yang disebut dengan ISAKMP/Oakley. *Framework* tersebut mencakup beberapa algoritma kriptografi yang telah ditentukan sebelumnya, dan juga dapat diperluas dengan menambahkan beberapa sistem kriptografi tambahan yang dibuat oleh pihak ketiga. Selama proses negosiasi dilakukan, persetujuan akan tercapai dengan metode autentikasi dan kemanan yang akan digunakan, dan protokol pun akan membuat sebuah kunci yang dapat digunakan bersama (shared key) yang

---

[102] Anonymous. http://www.wikipedia.org
[103] Anonymous. http://www.wikipedia.org

nantinya digunakan sebagi kunci enkripsi data. IPSec mendukung dua buah sesi komunikasi keamanan, yakni sebagai berikut:[104]

a) Protokol *Authentication Header* (AH), yakni menawarkan autentikasi pengguna dan perlindungan dari beberapa serangan (umumnya serangan *man in the middle*), dan juga menyediakan fungsi autentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima untuk merasa yakin bahwa identitas si pengirim adalah benar adanya, dan data pun tidak dimodifikasi selama transmisi. Namun demikian, protokol AH tidak menawarkan fungsi enkripsi terhadap data yang ditransmisikannya. Informasi AH dimasukkan ke dalam *header* paket IP yang dikirimkan dan dapat digunakan secara sendirian atau bersamaan dengan protokol *Encapsulating Security Payload*.
b) Protokol *Encapsulating Security Payload* (ESP), yakni protokol ini melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data. ESP juga dapat memiliki skema autentikasi dan perlindungan dari beberapa serangan dan dapat digunakan secara sendirian atau bersamaan dengan *Authentication Header*. Sama seperti halnya AH, informasi mengenai ESP juga dimasukkan ke dalam *header* paket IP yang dikirimkan.

Beberapa perangkat keras serta perangkat lunak dapat dikonfigurasikan untuk mendukung IPSec, yang dapat dilakukan dengan menggunakan enkripsi kunci publik yang disediakan oleh *Certificate Authority* (dalam sebuah *public key*

[104] Anonymous. http://www.wikipedia.org

infrastructure) atau kunci yang digunakan bersama yang telah ditentukan sebelumnya (skema *Pre-Shared Key*/PSK) untuk melakukan enkripsi secara privat.[105]

2.2.2.3.*Pretty Good Privacy (PGP)*

Pretty good privacy (PGP) adalah suatu perangkat lunak standar yang umum digunakan sebagai penyedia privasi di lingkungan Internet. Penggunaannya tergantung pada kepemilikan sepasang kunci, yang disebut *public key* dan *private key*. Salah satu cara yang umum digunakan untuk mempublikasikan *public key* dengan menyimpannya pada *Server Public key*. Informasi *public key* yang tersimpan pada server tersebut terdiri atas *public key* dan satu atau *lebih key identifier* dari *public key* tersebut. Identitas bagi kunci tersebut biasanya berupa alamat e-mail dari pemilik kunci yang bersangkutan.

Jika penggunaan alamat e-mail sebagai *key identifier* dijadikan sebagai suatu keharusan, maka memungkinkan digunakannya struktur domain dari elamat e-mail tersebut untuk membentuk suatu basis data *public key* yang tersusun secara hirarki. Dengan merestrukturisasi basis data *public key* secara hirarki dan memodifikasi perangkat lunak server *public key*, maka pencarian *public key* dapat dilakukan dengan memanfaatkan penggunaan struktur Internet *Domain Name System* (DNS). Pendekatan ini merupakan salah satu cara pendistribusian basis data *public key*.

Cara pendistribusian basis data *public key* secara hirarki tersebut selain dapat memecahkan masalah penyimpanan juga menghilangkan kebutuhan proses sinkronisasi antar *server public key*, seperti dibutuhkan pada metode yang

[105] http://www.wikipedia.org.

digunakan sekarang. Pengelolaan basis data juga menjadi lebih mudah karena dilakukan secara lokal. Agar pencarian lokasi pelayanan (server *public key*) dapat dilakukan dengan mudah dan efisien.[106]

2.2.2.4. Privacy Enhanced Mail (PEM)

Privacy-Enhanced Mail (PEM) merupakan standar internet yang aman untuk memberikan pertukaran surat elektronik. PEM menggunakan bebeberapa teknik kriptografi untuk kerahasiaan, otentifikasi pengirim, dan pesan integritas. Aspek integritas pesan yang memungkinkan pengguna untuk memastikan bahwa pesan belum diubah selama transportasi dari pengirim. Pengirim otentikasi memungkinkan pengguna untuk memverifikasi bahwa pesan PEM telah menerima bahwa mereka benar-benar dari orang yang mengklaim telah dikirim itu. Fitur kerahasiaan pesan yang akan disimpan rahasia dari orang-orang kepada siapa pesan itu tidak ditujukan.[107]

Menurut Linktionary, PEM adalah salah satu standar untuk pengamanan teks e-mail. PEM telah ditetapkan oleh IETF sebagai cara untuk mengenkripsi 7-bit pesan teks. Ia juga menetapkan struktur hirarkis untuk mendistribusikan dan verifikasi tanda tangan digital. PEM menetapkan prasarana publik-key untuk tombol tukar lebih besar jaringan seperti Internet. Namun, spesifikasi yang kurang lebih baru dan standar yang telah dikembangkan, seperti dibahas di bawah. [108]

---

106 Evi Irayani, *Pemanfaatan Resource Record DNS Tipe SRV dalam Pendistribusian Basis Data ublic key PGP*, Tesis, Fakultas Teknik Informatika ITS, Surabaya, 2007.

107 Michael A. Gurski Michael, *Privacy-Enhanced Mail (PEM)*, artikel. http://www.cs.umbc.edu/~woodcock/cmsc482/proj1/pem.html

108 Anonymous. http://www.linktionary.com

2.2.2.5. *Public key Cryptography Standards (PKCS)*

Kriptografi kunci publik adalah sebuah metode untuk komunikasi rahasia antara dua pihak tanpa memerlukan sebuah awal pertukaran kunci rahasia. Juga dapat digunakan untuk membuat tanda tangan digital. Kriptografi kunci publik yang mendasar dan banyak digunakan teknologi, dan memungkinkan aman transmisi informasi di Internet.

PKCS juga dikenal sebagai kriptografi asimetrik karena kunci yang digunakan untuk mengenkripsi pesan berbeda dari tombol digunakan mendekripnya itu. Dalam kriptografi kunci publik, pengguna memiliki sepasang kunci *cryptographic*, yakni sebuah kunci publik dan sebuah kunci pribadi. Kunci pribadi yang disimpan rahasia, sedangkan kunci publik dapat didistribusikan secara luas. Pesan yang terenkripsi dengan kunci publik penerima dan hanya dapat *decrypted* sesuai dengan kunci pribadi. Tombol terkait matematis, tetapi kunci pribadi praktis tidak dapat berasal dari kunci publik. Sebaliknya, rahasia-kunci kriptografi, juga dikenal sebagai kriptografi simetris, menggunakan satu rahasia kunci untuk enkripsi dan dekripsi. Untuk menggunakan kriptografi simetris untuk komunikasi, pengirim dan penerima harus berbagi kunci di muka.[109]

2.2.2.6. *Secure/Multipurpose Internet Mail Extensions (S/MIME)*

S/MIME adalah sebuah standar untuk kunci publik enkripsi dan menandatangani e-mail di *encapsulated* MIME. Pada awalnya dikembangkan oleh *RSA Data Security Inc* menggunakan spesifikasi baru yang dikembangkan IETF dengan spesifikasi standar industri *secure message format*.[110] Metode yang

[109] Anonymous. http://www.wikipedia.org
[110] Anonymous. http://www.wikipedia.org

digunakan dalam pengiriman e-mail yang menggunakan Rivest-Shamir-Adleman (RSA) enkripsi sistem. S/MIME termasuk dalam versi terbaru dari *Web browser* dari Microsoft dan Netscape dan juga telah didukung oleh vendor lainnya yang membuat pesan produk. S/MIME menjelaskan bagaimana enkripsi informasi digital dan sertifikat dapat dimasukkan sebagai bagian dari isi pesan.[111]

2.2.2.7. Secure Sockets Layer (SSL)

SLL adalah sebuah protokol yang dikembangkan oleh Netscape untuk transmisi dokumen pribadi melalui internet. SSL menggunakan sebuah *cryptographic* sistem yang menggunakan dua kunci untuk mengenkripsi data - kunci publik yang diketahui semua orang dan kunci rahasia pribadi atau hanya untuk diketahui penerima pesan. Netscape Navigator dan Internet Explorer keduanya mendukung SSL, dan banyak situs web menggunakan protokol untuk mendapatkan informasi rahasia pengguna, seperti nomor kartu kredit. URL yang memerlukan sebuah koneksi SSL mulai dengan *https*. Protokol lain untuk transmisi data secara aman melalui World Wide Web adalah *Secure HTTP (S-HTTP).* Sedangkan SSL membuat sambungan aman antara klien dan server, dimana setiap jumlah data yang dapat dikirim secara aman, S-HTTP adalah perangkat yang dirancang untuk mengirimkan pesan aman, karena itu, dapat dilihat sebagai komplementer daripada bersaing teknologi. Kedua protokol yang telah disetujui oleh *Internet Engineering Task Force* (IETF) sebagai standar.[112]

---

[111] Anonymous. http:// www.searchsecurity.com
[112] Lihat http://www.webopedia.com

2.2.2.8.*Transport Layer Security* (TLS)

Secure Socket Layer (SSL) dan *Transport Layer Security* (TLS), merupakan kelanjutan dari protokol *cryptographic* yang menyediakan komunikasi yang aman di Internet. Protokol ini menyediakan authentikasi akhir dan privasi komunikasi di Internet menggunakan kriptografi[113].

Dalam penggunaan umumnya, hanya server yang diautentikasi (dalam hal ini, memiliki identitas yang jelas) selama dari sisi client tetap tidak terauthentikasi. Authentikasi dari kedua sisi (mutual autentikasi) memerlukan penyebaran PKI pada *client*-nya. Protokol ini mengizinkan aplikasi dari client atau server untuk berkomunikasi dengan didesain untuk mencegah *eavesdropping*, *(tampering)* dan *message forgery*.[114]

Teknik-teknik kriptografi yang digunakan antara lain: fungsi *hash*, algoritma enkripsi simetrik, dan algoritma enkripsi asimetrik. Fungsi *hash* akan digunakan bersama dengan algoritma enkripsi asimetrik dalam bentuk tanda tangan elektronik untuk memastikan integritas dan keaslian berita/data berikut pengirimnya. Algoritma enkripsi simetrik digunakan untuk mengamankan data dengan cara enkripsi. Dalam PKI penggunaan algoritma enkripsi simetrik tidak langsung didefinisikan tetapi telah diimplementasikan oleh berbagai perangat lunak.[115]

Secara garis besar PKI diwujudkan dalam bentuk kolaborasi antar komponen-komponennya. Komponen-komponen PKI antara lain: *subscriber*,

---

[113] Ahmad Gunawan, *Posts filed under 'SSL & TLS(Transport Layer Security)*, 2007. http://kelasjarkom.wordpress.com

[114] Ahmad Gunawan, *ibid*.

[115] Ahmad Gunawan, *ibid*.

certification authority (CA), *registration authority* (RA), sertifikat elektronik. Secara praktis wujud PKI adalah penggunaan sertifikat elektronik. Sertifikat elektronik adalah sebuah file komputer yang berisi data-data tentang sebuah *public key*, pemiliknya (subscriber atau CA), CA yang menerbitkannya dan masa berlakunya. PKI telah diimplementasikan dengan berbagai aplikasi seperti S/MIME, HTTPS, VPN, dll. Anda dapat melihat fitur S/MIME pada software email yang terkenal seperti Outlook Express, Mozilla Mail/Thunderbird, dan Evolution.[116]

Protocol SSL dan TLS berjalan pada *layer* dibawah *application protocol* seperti HTTP, SMTP and NNTP dan di atas *layer* TCP *transport protocol*, yang juga merupakan bagian dari TCP/IP protokol. Selama SSL dan TLS dapat menambahkan keamanan ke protocol apa saja yang menggunakan TCP, keduanya terdapat paling sering pada metode akses HTTPS. HTTPS menyediakan keamanan *web-pages* untuk aplikasi seperti pada E-commerce. Protocol SSL dan TLS menggunakan kriptografi *public key* dan sertifikat *public key* untuk memastikan identitas dari pihak yang dimaksud. Sekarang juga sudah hampir seluruh perangkat internet seperti *browser* dan perangkat *client* atau *server side* yang sudah mendukung teknologi ini, seperti halnya ActiveX, SSL & TLS pada IE 7.0 yang sudah mulai bias dirasakan kenyamanannya.[117]

[116] Ahmad Gunawan, *ibid*.
[117] Ahmad Gunawan, *ibid*.